



Văn bằng Bitcoin

Giáo dục tài chính trong kỷ nguyên bitcoin

Sổ Tay Học Viên

Phiên Bản Tiếng Việt | 2025

Biên tập và lên kế hoạch: Seung-Goo Kang
Người dịch: Olivia Nguyễn

My First Bitcoin đã tạo ra tài liệu này và chia sẻ miễn phí theo giấy phép **Creative Commons**.

Tác phẩm này được cấp phép theo
Creative Commons
Attribution-ShareAlike
4.0 International (CC BY-SA 4.0)





Văn bằng Bitcoin

Giáo dục tài chính trong kỷ nguyên bitcoin

Sổ Tay Học Viên

Phiên Bản Tiếng Việt | 2025

Biên tập và lên kế hoạch: Seung-Goo Kang
Người dịch: Olivia Nguyễn



bc1q5es60qpa7gpkp0k32x14zefkj43kd9jxzdz54sgmv3y2r34dw8dqm9pzsdc

QUYỀN GÓP NGAU



Câu chuyện về Văn bằng Bitcoin

Không có gì mạnh mẽ hơn một ý tưởng đến đúng thời điểm.

Câu chuyện Văn bằng Bitcoin bắt đầu tại El Salvador, với chương trình thử nghiệm đầu tiên gồm 38 học sinh trường công lập tốt nghiệp vào tháng 6 năm 2022 — đây là Văn bằng Bitcoin đầu tiên trong hệ thống giáo dục công lập trên toàn thế giới.

Thật khó tin rằng điều đó xảy ra chưa đầy ba năm trước.

Kể từ đó, sự phát triển thật đáng kinh ngạc, với hàng ngàn học viên Văn bằng Bitcoin tốt nghiệp từ các lớp học trên khắp cả nước. Tuy nhiên, sự phát triển ấn tượng và truyền cảm hứng nhất lại đến từ những người khác. Cuốn sổ tay học tập này là mã nguồn mở, và một cộng đồng giáo viên Bitcoin vô cùng đa dạng đã đón nhận tài liệu này, cả ở El Salvador và tại nhiều nơi khác trên thế giới.

Bộ Giáo dục El Salvador đã sử dụng tài liệu này làm nội dung chính thức cho chương trình Văn bằng Bitcoin của mình. Vào năm 2024, chúng tôi đã hợp tác với Bitcoin Beach để đào tạo hơn 400 giáo viên trường công lập giảng dạy chương trình này tại trường của họ.

Một trong những mục tiêu đầu tiên của chúng tôi là giáo dục cả một quốc gia và bằng chứng rằng giáo dục về Bitcoin có thể trở thành một nguồn năng lượng tích cực trên quy mô lớn. Giấc mơ đó đang trên đà tiến tới thành hiện thực.

El Salvador là trọng tâm; sứ mệnh là toàn cầu.

Vào tháng 3 năm 2023, chúng tôi đã thành lập mạng lưới quốc tế Mạng lưới các nút giáo dục Bitcoin (Bitcoin Educators Node Network), yêu cầu tất cả các nút phải đồng thuận với một số nguyên tắc cốt lõi: giáo dục phải độc lập, khách quan, do cộng đồng dẫn dắt, chỉ tập trung vào Bitcoin, có chất lượng cao và hướng đến việc trao quyền. Mạng lưới này, hiện nay đã tự quản, đã dịch bộ tài liệu sang hơn tám ngôn ngữ và giảng dạy chương trình Văn bằng Bitcoin tại Canada, Hoa Kỳ, Mexico, Guatemala, Honduras, Costa Rica, Cuba, Cộng hòa Dominica, Haiti, Colombia, Suriname, Peru, Brazil, Argentina, Ireland, Vương quốc Anh, Bồ Đào Nha, Georgia, Ghana, Nigeria, Uganda, Kenya, Zambia, Zimbabwe, Nam Phi, Afghanistan, Bangladesh, Ấn Độ, Hồng Kông, Indonesia và Úc. Mạng lưới tiếp tục kết nạp thêm các nút mới mỗi tháng, và vì tài liệu là mã nguồn mở, không ai cần xin phép để sử dụng. Rất có thể còn nhiều người khác đã triển khai chương trình này hoàn toàn độc lập.

Đây là một phong trào toàn cầu, phi tập trung.

Giáo dục về Bitcoin độc lập, khách quan và do cộng đồng dẫn dắt sẽ làm thay đổi thế giới. Và điều đó đã bắt đầu.

Vì một thế giới tốt đẹp hơn,

Đội ngũ My First Bitcoin, 2025

Mục Lục

Chương #1: Tại sao chúng ta cần tiền?

1.0 Giới thiệu	01
1.1 Gặp Satoshi	01
Hoạt động: Năm câu hỏi về tiền	01
1.2 Thảo luận lớp – Tại sao chúng ta cần tiền?	04

Chương #2: Tiền là gì?

2.0 Giới thiệu	07
Hoạt động: Thảo luận lớp – “Tiền là gì?”	07
2.1 Định nghĩa về tiền	07
2.2 Chức năng của tiền	09
2.3 Tính chất của tiền	10
2.4 Các loại tiền	13
2.5 Tâm lý học về tiền: Sự khan hiếm, ưu tiên thời gian và sự đánh đổi	14
Hoạt động: Ưu tiên thời gian	16

Chương #3: Lịch sử của tiền

3.0 Giới thiệu	21
Hoạt động: Trò chơi đổi chác	21
3.1 Tiến hóa từ đổi chác đến tiền tệ hiện đại	23
3.1.1 Những vấn đề với các hình thức tiền sơ khai	23
3.1.2 Sự phát triển của tiền xu và tiền giấy	24
3.1.3 Chuyển đổi từ tiền vững chắc sang tiền không vững chắc	25
3.1.4 Từ giấy đến nhưa	27
3.2 Tiền kỹ thuật số	28

Chương #4: Tiền pháp định là gì và ai kiểm soát nó?

4.0 Giới thiệu	31
4.1 Lược sử về tiền pháp định	31
4.2 Hệ thống tiền pháp định	34
4.2.1 Hệ thống tiền tệ theo nghị định	34

4.2.2 Ngân hàng dự trữ một phần: hệ thống được thúc đẩy bởi nợ	35
Hoạt động: Ngân hàng dự trữ một phần	38
4.2.3 Ai kiểm soát hệ thống tiền pháp định và họ hưởng lợi ra sao?	39
4.3 Tiền kỹ thuật số của ngân hàng trung ương: Tương lai của tiền pháp định	41

Chương #5: Làm thế nào vấn đề dẫn đến giải pháp

5.0 Giới thiệu về vấn đề	45
5.1 Sức mua giảm sút	45
5.1.1 Lạm phát tiền tệ và tác động đến sức mua	45
Hoạt động: Tác động của lạm phát — hoạt động đấu giá	46
5.2 Gánh nặng nợ toàn cầu và bất bình đẳng xã hội	47
5.2.1 Tác động đến cá nhân — mất sức mua	47
5.2.2 Tác động xã hội — bất bình đẳng giàu nghèo tăng	52
Hoạt động: Hậu quả của hệ thống tiền pháp định	53
5.2.3 Gánh nặng nợ toàn cầu	54
5.3 Những Cypherpunk và hành trình tìm kiếm tiền tệ phi tập trung	55
5.3.1 Những Cypherpunk	56
5.3.2 Hệ thống tập trung và phi tập trung	57
5.3.3 Lược sử về tiền kỹ thuật số	59

Chương #6: Giới thiệu về Bitcoin

6.0 Satoshi Nakamoto và sự ra đời của Bitcoin	63
6.1 Bitcoin hoạt động như thế nào?	65
6.1.1 Cơ chế đồng thuận Nakamoto (Nakamoto Consensus)	65
6.1.2 Những người chơi trò chơi	67
Hoạt động: Xây dựng đồng thuận trong mạng ngang hàng	69
6.2 Bitcoin như tiền kỹ thuật số có giá trị thực	71
6.2.1 Giới thiệu	71
6.2.2 Đặc điểm của Bitcoin	72
Hoạt động: Thảo luận lớp — Bitcoin có phải là tiền vững chắc không?	76
6.2.3 Chấp nhận trách nhiệm cá nhân	76

Chương #7: Cách sử dụng Bitcoin

7.0 Giới thiệu	81
7.1 Mua và trao đổi Bitcoin	81
7.1.1 Giao dịch ngang hàng (P2P): Trực tiếp	81
7.1.2 Giao dịch ngang hàng (P2P): Trực tuyến	82
7.1.3 Sàn giao dịch tập trung	82
7.2 Giới thiệu về ví Bitcoin	83
7.2.1 Ví tự lưu ký và ví lưu ký	83
7.2.2 Các loại ví Bitcoin khác nhau	85
7.2.3 Mã nguồn mở và mã nguồn đóng	86
Hoạt động: Đánh giá ví Bitcoin trong lớp học	87
7.3 Thiết lập ví bitcoin di động	87
Hoạt động: Thiết lập và khôi phục ví Bitcoin	87
7.4 Nhận và gửi giao dịch	89
Hoạt động: Giao dịch Bitcoin trong thực tế	91
7.5 Tiết kiệm bằng Bitcoin	93
7.6 Đừng tin, hãy xác minh	94

Chương #8: Lightning Network: Sử dụng Bitcoin trong đời sống hằng ngày

8.0 Giới thiệu	97
Hoạt động: Xem "Giải thích Lightning Network của Bitcoin: Cách nó hoạt động thực sự"	98
8.1 Lightning Network	98
8.2 Các loại ví Lightning khác nhau	100
8.2.1 Ví tự lưu ký và ví lưu ký	100
8.2.2 Mã nguồn mở và mã nguồn đóng	100
8.3 Thiết lập ví Lightning Bitcoin	100
8.4 Gửi và nhận giao dịch Lightning	102
Hoạt động: Cuộc đua tiếp sức ví Lightning	106
8.5 Mua cà phê và hàng tạp hóa bằng Bitcoin	107
8.5.1 Trực tuyến: Plugin thanh toán — Thương mại điện tử	108
8.5.2 Trực tiếp: Tìm thương nhân trong khu vực của bạn	109
8.5.3 Công cụ chuyển tiếp: Thẻ quà tặng và Thẻ thanh toán	110
8.5.4 Kinh tế tuần hoàn và Bitcoin như một phương tiện trao đổi	110

Chương #9: Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.0 Giới thiệu	115
Hoạt động: Xem “Cách Bitcoin hoạt động bên trong”	115
9.1 Khóa công khai và khóa riêng: Bảo mật thông qua mật mã học	116
9.1.1 Mật mã học khóa công khai và khóa riêng	116
9.1.2 Giải thích hàm băm	119
Hoạt động: Tạo mã băm SHA-256	121
9.2 Mô hình UTXO	122
9.3 Nhìn kỹ hơn vào các nút Bitcoin và thợ đào	125
9.3.1 Nút Bitcoin là gì và cách làm thế nào để thiết lập một nút?	125
Hoạt động: Xem video về các nút Bitcoin	126
9.3.2 Thợ đào Bitcoin là gì và quá trình đào hoạt động như thế nào?	126
9.4 Mempool là gì?	132
Hoạt động: Mempool	134
9.5 Quy trình hoạt động của một giao dịch Bitcoin từ đầu đến cuối	135

Chương #10: Tại sao Bitcoin?

10.0 Giới thiệu	139
Hoạt động: Tương lai của Bitcoin có thể trông như thế nào?	139
10.1 Tiền kỹ thuật số của ngân hàng trung ương (CBDC) là gì và ai kiểm soát chúng?	140
10.2 Triết lý của Bitcoin	141
Hoạt động: Thảo luận lớp — Bạn có quyền kiểm soát tiền của chính mình không?	141
10.3 Lợi ích của Bitcoin	142
10.4 Một tương lai được trao quyền	143
Hoạt động: Thảo luận lớp — Quan điểm của bạn đã thay đổi như thế nào?	143
Tài nguyên bổ sung	147
Khái niệm chính của chương	149
Bảng thuật ngữ	153

Văn bằng Bitcoin

*Hành trình chuyển hóa kéo dài 10 tuần
qua nền giáo dục độc lập, khách
quan, chất lượng cao và miễn phí*

Điều cần thiết là phải nắm vững kiến thức cơ bản về tiền, lịch sử của nó và hệ thống tài chính hiện tại trước khi nghiên cứu [Bitcoin](#). Việc hiểu rõ những khái niệm này sẽ tạo nền tảng vững chắc giúp bạn thấu hiểu bản chất độc đáo và mang tính đột phá của [Bitcoin](#). Qua việc tìm hiểu quá trình tiến hóa của tiền, bạn sẽ có khả năng nhận thức rõ hơn về tiềm năng cũng như hạn chế của hệ thống tài chính hiện tại, đồng thời hiểu cách Bitcoin hướng tới giải quyết những hạn chế đó. Thiếu đi nền tảng này, bạn có thể gặp khó khăn trong việc đánh giá đầy đủ tầm quan trọng và tác động tiềm năng của Bitcoin. Hãy tin tưởng vào quá trình học tập và giữ vững sự tập trung, bởi phần thưởng cho sự hiểu biết sâu sắc và sự đánh giá cao lĩnh vực tiên tiến này sẽ vô cùng xứng đáng.

Chương #1

Tại sao chúng ta cần tiền?

1.0 Giới thiệu

1.1 Gặp Satoshi

Hoạt động: Năm câu hỏi về tiền

1.2 Thảo luận lớp – Tại sao chúng ta cần tiền?

Tại sao chúng ta cần tiền?

1.0 Giới thiệu

Tiền là một trong những công cụ vĩ đại nhất của tự do mà con người đã phát minh ra.

Friedrich Hayek

Chào mừng bạn đến với Văn bằng Bitcoin. Trong chương này, chúng ta sẽ khám phá câu hỏi cơ bản về lý do tại sao tiền lại cần thiết trong cuộc sống của chúng ta. Chúng ta sẽ tìm hiểu bản chất của tiền và các hình thức khác nhau của nó, nhằm hiểu sâu hơn về tầm quan trọng của tiền. Tiền là thứ mà chúng ta sử dụng gần như mỗi ngày, nhưng liệu chúng ta có thực sự hiểu tại sao chúng ta cần nó và nó là gì không? Tại sao cha mẹ và các thành viên khác trong gia đình lại đánh đổi thời gian của họ để lấy tiền? Tại sao một số người có nhiều tiền hơn những người khác? Tại sao tiền lại khác nhau ở các quốc gia khác? Tại sao chúng ta không thể chỉ tạo ra thêm tiền khi cần?

1.1 Gặp Satoshi



Xin chào! Tôi là Satoshi, trợ lý tương tác sẽ đồng hành cùng bạn trong suốt khóa học Văn bằng Bitcoin. Tôi sẽ cung cấp các tài nguyên và gợi ý hữu ích để bạn có thể tìm hiểu kỹ hơn về các khái niệm chính.



Hoạt động: Chúng ta hãy bắt đầu chương này bằng cách trả lời năm câu hỏi dưới đây

Hãy xem xét các cách sử dụng thực tế, chẳng hạn như mua các nhu yếu phẩm như thực phẩm và những món đồ bạn mong muốn. Hãy cố gắng đưa ra các ví dụ cụ thể, kết hợp sự sáng tạo với tính thực tế.

Chương #1



Tại sao chúng ta cần tiền?

Tiền là gì?

Tại sao chúng ta cần tiền?

Ai kiểm soát tiền?

Điều gì tạo nên “giá trị” của tiền?

Bạn có thắc mắc gì về tiền bạc? Hãy viết câu hỏi của bạn ở đây để chia sẻ với lớp.

Mở rộng cuộc thảo luận ra toàn lớp, chia sẻ và so sánh các danh sách để xác định năm lý do thiết yếu nhất cho việc cần đến tiền. Xác định những ý tưởng chung trong lớp. Suy ngẫm về những ý tưởng độc đáo của riêng bạn không có trong danh sách nhưng vẫn đáng cân nhắc. Ghi lại những suy nghĩ bổ sung này.

1.2 Thảo luận lớp — Tại sao chúng ta cần tiền?

Lớp sẽ chia thành các nhóm và:

-  Chia sẻ và thảo luận câu trả lời cho bốn câu hỏi đầu tiên. Viết lại câu trả lời yêu thích của nhóm.
-  Chia sẻ câu trả lời cho câu hỏi cuối cùng và bình chọn một câu hỏi học sinh yêu thích nhất. Viết lại kết quả.
-  Xem lại các câu trả lời và câu hỏi này vào cuối Văn bằng Bitcoin.

Bây giờ bạn đã hiểu rõ hơn về lý do tại sao tiền lại cần thiết, các chương tiếp theo sẽ khám phá tiền là gì, cách tiền phát triển theo thời gian, ai ảnh hưởng đến nó, và hình thức mới nhất của tiền. Hãy tiếp tục tham khảo danh sách bạn đã lập từ ngày đầu tiên trong lớp để nối kết những hiểu biết của bạn với sự phát triển trong cách tạo ra, định nghĩa và sử dụng tiền qua các thời kỳ.

Chương #2

Tiền là gì?



2.0 Giới thiệu

Hoạt động: Thảo luận lớp – “Tiền là gì?”

2.1 Định nghĩa về tiền

2.2 Chức năng của tiền

2.3 Tính chất của tiền

2.4 Các loại tiền

2.5 Tâm lý học về tiền: Sự khan hiếm, ưu tiên thời gian và sự đánh đổi

Hoạt động: Ưu tiên thời gian

Tiền là gì?

2.0 Giới thiệu

Tiền là một sự đảm bảo rằng chúng ta có thể có được những gì mình muốn trong tương lai. Mặc dù hiện tại chúng ta không cần gì, nhưng tiền đảm bảo khả năng thỏa mãn những mong muốn mới khi chúng phát sinh.

Aristotle

Tiếp nối việc khám phá vì sao tiền lại cần thiết, chương này sẽ tìm hiểu câu hỏi cốt lõi: Tiền là gì? Chúng ta sẽ bắt đầu với một cuộc thảo luận và hoạt động nhóm.

Hoạt động: Thảo luận lớp – “Tiền là gì?”

- 💡 Xin đừng ăn kẹo được đặt trên bàn của bạn ngay bây giờ.
- 💡 Ai sẵn sàng đổi viên kẹo của mình lấy một tờ tiền 1 đô la Mỹ?
- 💡 Bây giờ, hãy giữ tay giơ lên nếu bạn vẫn sẵn sàng đổi viên kẹo của mình lấy một tờ tiền 1 đô la Cờ tỷ phú thay vào đó.
- 💡 Tại sao hoặc tại sao không?
- 💡 Vì sao một tờ tiền có giá trị, còn tờ khác lại vô giá trị?
- 💡 Điều gì mang lại “giá trị” cho tiền?
- 💡 Tiền có nguồn gốc từ đâu, và ai là người quyết định in bao nhiêu tiền?
- 💡 Tại sao không in thêm tiền và phân phối đều cho mọi người?

Điểm khác biệt duy nhất giữa hai tờ tiền này là niềm tin của bạn rằng một tờ có giá trị hơn tờ kia.



2.1 Định nghĩa về tiền

Bạn đã bao giờ dừng lại để suy nghĩ xem tiền thực sự là gì chưa? Bạn có bao giờ tự hỏi điều gì khiến tiền... trở thành “tiền”? Hầu hết chúng ta đều biết cách sử dụng tiền, nhưng không nhiều người hiểu tiền đến từ đâu hoặc nó hoạt động như thế nào. Về cơ bản, tiền là một phương tiện để trao đổi hàng hóa và dịch vụ. Nó đại diện cho giá trị của những thứ này dưới một hình thức có thể dễ dàng giao dịch. Hình thức đó có thể là tiền giấy, tiền xu hoặc thanh toán điện tử. Chính phủ hoặc các cơ quan có thẩm quyền thường phát hành và kiểm soát tiền, nhưng tiền còn hơn cả một phương tiện trao đổi vật lý hay kỹ thuật số. Nó giống như một ngôn ngữ chung giúp chúng ta giao thương với mọi người trên khắp thế giới, ngay cả khi không nói cùng một ngôn ngữ hay chia sẻ cùng một nền văn hóa. Ví dụ, bạn có thể đang ở phía bên kia thế giới nhưng vẫn có thể “nói chuyện bằng tiền” bằng cách đặt một món hàng lên quầy và đổi lấy tiền địa phương, hoặc quét thẻ tín dụng để thanh toán.

Chương #2

Tiền giống như một hợp đồng xã hội cho phép chúng ta trao đổi mà không cần phải dựa vào hình thức đổi chác hoặc tìm ai đó đang cần đúng thứ mà ta có. Nếu một nhóm người bắt đầu chấp nhận sô cô la để thanh toán cho hầu hết hàng hóa và dịch vụ, thì sô cô la sẽ trở thành tiền (mặc dù vì dễ bị chảy ở một số nơi trên thế giới, có lẽ đó sẽ là một loại tiền không lý tưởng).

Như nhà kinh tế học người Pháp Jean-Baptiste Say đã chỉ ra: "Tiền chỉ thực hiện một chức năng nhất thời trong quá trình trao đổi; và khi giao dịch kết thúc, người ta sẽ thấy rằng một loại hàng hóa đã được trao đổi lấy một loại hàng hóa khác."

Nói cách khác, bản thân tiền không thể đáp ứng nhu cầu của con người; nó chỉ là một công cụ giúp chúng ta trao đổi hàng hóa này lấy hàng hóa khác.



Giao dịch là việc trao đổi hoặc chuyển giao hàng hóa và dịch vụ. Đây là cách trao đổi giá trị giữa hai hoặc nhiều bên.

Có nhiều loại giao dịch khác nhau, từ các giao dịch đơn giản (chẳng hạn như mua một chiếc bánh mì ở tiệm bánh mì) đến những giao dịch tài chính phức tạp hơn (như mua nhà hoặc đầu tư vào cổ phiếu hoặc trái phiếu). Các giao dịch có thể được thực hiện trực tiếp, qua điện thoại, trực tuyến hoặc bằng các hình thức khác, và có thể bao gồm nhiều bên tham gia, trong đó có cá nhân, doanh nghiệp và các tổ chức tài chính.



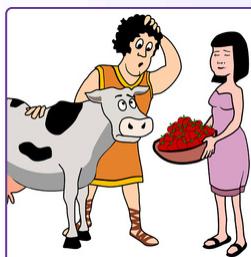
Hãy xem đoạn video ngắn này!



Không có tiền, việc trao đổi này sẽ dễ dàng hay khả thi đến mức nào?

Bạn có sẵn sàng đổi một con bò lấy 1 triệu quả dâu tây không?

Hay 600.000 quả? Còn 50.000 quả thì sao?



Tiền **LÀ** giá trị **BẮNG** đó hàng hóa được trao đổi.
Tiền **KHÔNG PHẢI** là giá trị **ĐỂ LẤY** hàng hóa được trao đổi.

Tóm lại, tiền:

Giúp các giao dịch trở nên dễ dàng vì ai cũng chấp nhận nó như một khoản thanh toán cuối cùng. Tiền cũng cho phép chúng ta đo lường giá trị và so sánh các hàng hóa, dịch vụ khác nhau. Tiếp theo, chúng ta sẽ tìm hiểu về chức năng của tiền.

Tiền là gì?

2.2 Chức năng của tiền

Khi nói đến việc mua bán hàng hóa và dịch vụ, tiền đóng vai trò chủ đạo. Tiền đảm nhận nhiều chức năng quan trọng, chẳng hạn như:

1

Cất trữ giá trị

Tiền nên giữ được giá trị theo thời gian, giúp nó trở thành phương tiện hữu ích để tiết kiệm và đầu tư giá trị của sức lao động con người. Điều này cho phép mọi người sử dụng tiền để lập kế hoạch cho tương lai, cũng như vay và cho vay. Vì vậy, lần tới khi bạn đang tiết kiệm cho một điều gì đó đặc biệt, hãy nhớ rằng tiền không chỉ là cách để thanh toán — mà còn là công cụ giúp bạn lên kế hoạch và đầu tư cho tương lai.

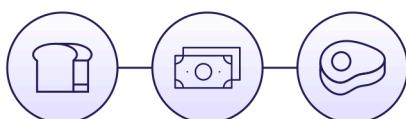
Cất trữ giá trị của bạn là gì?	BTC (USD)	Vàng (USD)	USD (EUR)
14 Tháng 3, 2019	3.846 USD	1.293 USD	0,8817 EUR
14 Tháng 3, 2020	5.258 USD	1.529 USD	0,90056 EUR
Lãi/Lỗ	+36,71%	+18,25%	+2,14%

2

Phương tiện trao đổi

Với tiền, bạn không cần phải tìm người muốn chính xác thứ bạn đang có để trao đổi. Thay vào đó, bạn có thể sử dụng tiền để mua và bán bất cứ thứ gì bạn muốn. Điều này giúp việc trao đổi và thương mại trở nên thuận tiện và hiệu quả hơn rất nhiều.

Phương tiện trao đổi



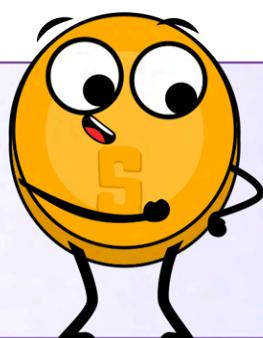
3

Đơn vị hạch toán

Tiền cung cấp một chuẩn mực giá trị chung, cho phép mọi người biểu đạt và so sánh giá của các hàng hóa và dịch vụ khác nhau. Điều này giúp thị trường trở nên hiệu quả và minh bạch hơn, nơi mọi người có thể đưa ra quyết định sáng suốt về việc mua và bán.

Đơn vị hạch toán

Người tiêu dùng biết giá trị của một thứ gì đó khi bạn gắn một mức giá (giá trị tiền tệ) cho nó.



29,00 USD

350,00 USD

Hãy nghĩ như thế này: nếu bạn muốn mua một chiếc xe mới, bạn có thể so sánh giá từ các đại lý khác nhau và đưa ra quyết định sáng suốt về việc nên mua chiếc nào dựa trên giá trị bằng đồng đô la. Nếu không có đơn vị换算, bạn sẽ phải cố gắng so sánh giá trị của một chiếc xe với chiếc khác bằng cách dùng những thứ khác, chẳng hạn như số lượng bò mà nó có giá trị hoặc thời gian để sản xuất chiếc xe đó.

Ba chức năng này là những yếu tố cho phép nền kinh tế trở nên phức tạp và năng động. Nếu không có tiền, việc mua bán hàng hóa và dịch vụ sẽ khó khăn hơn rất nhiều, và nền kinh tế của chúng ta cũng kém phát triển hơn.

Bài tập trên lớp — Đây là ví dụ cho chức năng nào của tiền?

-  Evan quyết định tiết kiệm một phần tiền lương hàng tuần của mình để mua một con chó con.
-  Adam mua hai miếng pizza với giá 8,30 đô tại tiệm Ray's Pizza.
-  Marc không thể quyết định nên mua vé hòa nhạc giá 75 đô la hay mua thẻ trượt tuyết giá 95 đô la.

2.3 Tính chất của tiền

Theo thời gian, con người dần nhận ra rằng tiền phải có một số đặc điểm nhất định để hoạt động hiệu quả như một phương tiện trao đổi. Những đặc điểm đó bao gồm tính lâu bền, tính chia nhỏ, tính dễ mang theo, tính chấp nhận, tính khan hiếm và tính thay thế.

 **Tính lâu bền** đề cập đến khả năng của tiền trong việc chống lại sự hao mòn vật lý và tồn tại lâu dài theo thời gian. Điều này đảm bảo tiền có thể lưu thông trong nền kinh tế ở trạng thái được chấp nhận và dễ nhận biết. Vàng là một chất liệu bền bỉ, có thể chịu được mài mòn và hư hại, nên là một ví dụ tiêu biểu cho đặc tính tính lâu bền của tiền.



 **Tính chia nhỏ** đề cập đến việc tiền có thể được phân thành các đơn vị nhỏ hơn, giúp mọi người có thể sử dụng để mua các mặt hàng với các số tiền khác nhau. Tiền giấy dễ dàng chia thành các mệnh giá nhỏ hơn, vì vậy nó là minh chứng tốt cho đặc tính khả năng chia nhỏ của tiền.



Tiền là gì?



Tính dễ mang theo đề cập đến mức độ dễ dàng vận chuyển và mang theo tiền. Điều này cho phép mọi người sử dụng tiền để mua bán hàng hóa và dịch vụ mà không gặp khó khăn. Tính dụng có tính dễ mang theo cao vì có thể dễ dàng mang trong ví hoặc túi xách, làm cho chúng trở thành ví dụ điển hình cho đặc điểm này của tiền.



Tính chấp nhận đề cập đến mức độ tiền được chấp nhận rộng rãi như một hình thức thanh toán, giúp mọi người có thể mua bán hàng hóa và dịch vụ một cách tự tin. Đồng đô la Mỹ được chấp nhận rộng rãi như một phương tiện thanh toán, khiến nó trở thành một ví dụ tiêu biểu cho đặc điểm chấp nhận của tiền.



Tính khan hiếm đề cập đến nguồn cung tiền có hạn, giúp duy trì giá trị của tiền và ngăn chúng ta phải chi nhiều tiền hơn để mua cùng một lượng hàng hóa. Tem sưu tập, đặc biệt là những con tem hiếm và có giá trị, có thể là một hình thức tiền tốt vì chúng khan hiếm và có thể tăng giá trị theo thời gian. Những người sưu tập tem thường dùng bộ tem của mình như một cách để đầu tư tài sản và đa dạng hóa danh mục đầu tư.



Tính thay thế đề cập đến khả năng thay thế cho nhau của tiền, sao cho một đơn vị tiền tương đương với đơn vị khác cùng giá trị. Tiền nên đồng nhất. Đồng tiền đồng có kích thước và trọng lượng đồng đều, khiến chúng trở thành một ví dụ tốt cho đặc điểm đồng nhất của tiền. Một xu luôn luôn là một xu.



Nhìn chung, những đặc điểm này khiến tiền trở thành một công cụ hữu ích và hiệu quả trong việc thúc đẩy giao dịch và thương mại, và chúng đóng vai trò thiết yếu đối với sự phát triển và ổn định kinh tế.

Bài tập trên lớp

Các loại tài sản khác nhau có những tính chất của tiền khác nhau và thực hiện các chức năng của tiền ở các mức độ khác nhau. Xã hội cuối cùng sẽ quyết định tài sản nào được sử dụng làm tiền dựa trên các yếu tố như tính ổn định, tính khan hiếm, tính chia nhỏ, tính chuyển nhượng và tính chấp nhận như một phương tiện trao đổi.

Để xác định mức độ phù hợp của các vật thể khác nhau với các tính chất cụ thể của tiền, bạn có thể chấm điểm từng vật theo thang điểm từ **1** đến **5** cho mỗi tính chất. Bằng cách cộng điểm cho từng vật, bạn có thể xác định vật nào phù hợp nhất để trở thành một hình thức tiền tệ.

[**0 = Tệ; 3 = Tạm được; 5 = Xuất sắc**]

***Vui lòng không điền vào cột dành cho Bitcoin; chúng ta sẽ quay lại phần này sau trong khóa học.**

Sử dụng các câu hỏi sau để giúp xác định mức độ phù hợp của các mục trong bảng với các tính chất của tiền.

-  **Tính lâu bền:** Tiền có thể chịu được hao mòn theo thời gian không?
-  **Tính dễ mang theo :** Tiền có thể dễ dàng vận chuyển và sử dụng ở nhiều địa điểm khác nhau không?
-  **Tính thay thế:** Tiền này có thể được hoán đổi với các hình thức tiền khác hay không?
-  **Tính chấp nhận:** Tiền có được chấp nhận rộng rãi như một hình thức thanh toán không?
-  **Tính khan hiếm:** Tiền có khan hiếm và không quá dư thừa không?
-  **Tính chia nhỏ:** Tiền có thể chia nhỏ thành các đơn vị nhỏ hơn để thực hiện giao dịch không?

Đặc điểm của tiền tốt					
Bền					
Dễ mang theo					
Đồng nhất					
Được chấp nhận					
Khan hiếm					
Chia nhỏ					
Tổng					

Tiền là gì?

2.4 Các loại tiền

Tiền có thể được chia thành hai loại chính: tiền vật lý và tiền kỹ thuật số.

Tiền vật lý bao gồm:

- ☀ Tiền pháp định là các tờ tiền giấy và đồng xu do chính phủ phát hành và được chấp nhận như một phương tiện trao đổi.
- ☀ Tiền đại diện là loại tiền đại diện cho quyền yêu cầu đối với một hàng hóa vật chất.
- ☀ Tiền hàng hóa là vật thể vật lý có giá trị nội tại và được chấp nhận rộng rãi như một phương tiện trao đổi — ví dụ như vàng và bạc.



**Không phải tất cả
tiền đều giống nhau!**



Tiền hàng hóa



Những vật như thuốc súng này từng được dùng làm tiền hàng hóa.

Tiền đại diện



Tiền đại diện như chứng chỉ bạc này có thể được đổi lấy bạc thật.

Tiền pháp định



Ngày nay, tiền giấy của Cục Dự trữ Liên bang là tiền pháp định, được chính phủ liên bang tuyên bố là phương tiện thanh toán hợp lệ.



Mặt khác, **tiền kỹ thuật số** có thể được sử dụng cho các giao dịch trực tuyến và bao gồm tiền điện tử, stablecoin, và tiền mã hóa.

Tiền điện tử là phiên bản kỹ thuật số của tiền thông thường, như đô la hoặc euro, và có thể được dùng để mua bán trực tuyến qua các **hệ thống thanh toán kỹ thuật số**.



Hệ thống thanh toán kỹ thuật số là cơ sở hạ tầng cho phép di chuyển tiền điện tử và các tài sản kỹ thuật số khác từ nơi này đến nơi khác. Tuy nhiên, trong hệ thống tài chính truyền thống, luôn có một bên trung gian, chẳng hạn như ngân hàng hoặc tổ chức tài chính khác, thu phí và có thẩm quyền chấp nhận, hủy, hoàn lại hoặc trì hoãn giao dịch.

Trong hệ thống tài chính trung gian, các loại hệ thống thanh toán kỹ thuật số chính bao gồm mạng lưới thẻ — giúp chuyển tiền giữa các tổ chức tài chính và thương nhân khi khách hàng thực hiện giao dịch bằng thẻ ghi nợ hoặc thẻ tín dụng — và ví điện tử, là các tài khoản trực tuyến cho phép người dùng lưu trữ và quản lý tiền điện tử của họ cũng như thực hiện thanh toán bằng cách chuyển tiền từ tài khoản của mình sang tài khoản người nhận.



Tiền kỹ thuật số của ngân hàng trung ương (CBDC)

Phiên bản kỹ thuật số của tiền pháp định của một quốc gia, được phát hành và bảo đảm bởi ngân hàng trung ương, đồng thời được điều phối thông qua các cơ quan chính phủ.



Stablecoin (Tiền ổn định giá)

Tiền kỹ thuật số được thiết kế để duy trì giá trị ổn định so với một tài sản, chẳng hạn như đồng đô la Mỹ.



Tiền mã hoá

Một loại tiền kỹ thuật số. Một số tiền mã hoá hoạt động phi tập trung và được quản lý bởi các quy tắc, trong khi một số khác được tập trung và kiểm soát bởi một nhóm người nhỏ.

Cuối cùng, một loại tiền tệ vận hành mà không cần bên trung gian sẽ hiệu quả hơn và mang lại lợi ích cho xã hội, vì nó ngăn chặn việc một vài cá nhân kiểm soát nguồn cung tiền và tập trung quyền lực. Tuy nhiên, việc tạo ra một loại tiền tệ như vậy, cho phép thực hiện các giao dịch an toàn mà không dựa vào sự tin cậy giữa các bên, đã là một thách thức trong suốt lịch sử. Để đạt được điều này, cần phải tạo ra một loại tiền tệ hoạt động giống như Internet, nơi quyền kiểm soát được phân phối cho tất cả mọi người nhưng lại không thuộc về riêng ai. Điều này đòi hỏi sự đồng thuận của tất cả các bên, bao gồm cả những người đang nắm quyền lực, để từ bỏ quyền kiểm soát vì lợi ích chung.

2.5 Tâm lý học về tiền: Sự khan hiếm, ưu tiên thời gian và sự đánh đổi

Giả sử bạn bị mắc kẹt giữa sa mạc và chỉ còn một chai nước duy nhất. Bạn đang rất khát và tuyệt vọng muốn uống, nhưng bạn cũng biết rằng mình cần phải giữ nước để tồn tại cho đến khi tìm được nguồn nước khác. Đây là một ví dụ điển hình về sự khan hiếm — bạn chỉ có một lượng tài nguyên hạn chế (nước) và phải đưa ra quyết định về cách sử dụng nó. Trong tình huống này, bạn có thể quyết định chia nhỏ nước và uống từng ngụm nhỏ trong thời gian dài nhất có thể để kéo dài thời gian sử dụng.

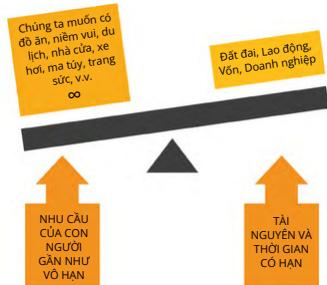
Tiền là gì?



Sự khan hiếm buộc chúng ta phải cân nhắc ưu và nhược điểm của cách sử dụng tài nguyên và đưa ra các lựa chọn đánh đổi.

Ngoài ra, bạn có thể quyết định uống hết lượng nước còn lại trong một lần, hy vọng cơn khát được giải tỏa sẽ giúp bạn có đủ năng lượng để tìm thêm nước. Dù chọn phương án nào, bạn cũng phải đổi mới với một quyết định khó khăn. Trong trường hợp này, lựa chọn nằm giữa việc giải tỏa cơn khát ngay lập tức và giữ nước để dùng về sau. Khái niệm khan hiếm này áp dụng cho mọi loại tài nguyên, không chỉ riêng nước. Dù đó là tiền bạc, thời gian, hay thậm chí là tình yêu và sự quan tâm, chúng ta luôn phải đưa ra quyết định về cách phân bổ nguồn lực hạn chế của mình.

Có hai loại sự khan hiếm: do con người tạo ra và tự nhiên.



💡 **Sự khan hiếm** do con người tạo ra, còn được gọi là **sự khan hiếm tập trung**, bao gồm những thứ như túi hàng hiệu phiên bản giới hạn, thẻ thể thao hiếm và các tác phẩm nghệ thuật có đánh số. Những thứ này dễ bị sao chép hoặc làm giả.

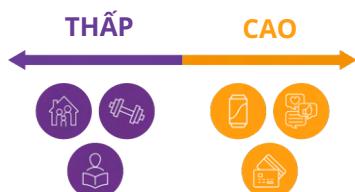
💡 **Sự khan hiếm** tự nhiên, còn được gọi là **sự khan hiếm phi tập trung**, bao gồm những thứ như muối, vỏ sò và các kim loại quý như vàng. Những thứ này khó sao chép hoặc làm giả hơn. Sự khác biệt chính giữa hai loại là **sự kiểm soát**.

Sự khan hiếm tập trung được kiểm soát bởi một thực thể duy nhất, như một công ty hoặc chính phủ, trong khi sự khan hiếm phi tập trung không bị ai kiểm soát. Một ví dụ về sự khan hiếm tập trung ảnh hưởng không tương xứng đến người nghèo là việc kiểm soát các nguồn tài nguyên thiết yếu như nước sạch. Ở một số khu vực, việc tiếp cận nước sạch được quản lý bởi các công ty tư nhân hoặc cơ quan nhà nước, có thể hạn chế việc phân phối nước, dẫn đến sự khan hiếm nguồn tài nguyên quan trọng này. Việc kiểm soát tập trung này có thể dẫn đến tăng giá hoặc tiếp cận không đồng đều với nước sạch, khiến các cộng đồng nghèo đói thường phải gánh chịu hậu quả nặng nề nhất. Việc tiếp cận hạn chế với nước sạch không chỉ ảnh hưởng đến sức khỏe và đời sống của họ mà còn kéo dài tình trạng nghèo đói vì họ có thể phải trả giá cao hơn hoặc phải đi xa để lấy nước.

Sự khan hiếm ảnh hưởng đến các lựa chọn của chúng ta. Hiểu được điều này có thể giúp cải thiện khả năng ra quyết định. Chúng ta thường phải lựa chọn giữa lợi ích trước mắt và lợi ích lâu dài, và những sự đánh đổi này định hình con đường chúng ta đạt được mục tiêu của mình.



Ưu tiên thời gian đề cập đến ý tưởng rằng con người thường thích có được một thứ gì đó NGAY BÂY GIỜ hơn là về sau.



Một ví dụ về ưu tiên thời gian:

Giả sử bạn có lựa chọn nhận 100 đô la ngay hôm nay hoặc 110 đô la sau một năm. Nếu bạn có ưu tiên thời gian cao, bạn có thể chọn nhận 100 đô la ngay hôm nay vì bạn coi trọng việc có 100 đô la ngay bây giờ hơn là lợi ích của việc chờ thêm một năm để nhận thêm 10 đô la. Mặt khác, nếu bạn có ưu tiên thời gian thấp, bạn sẽ chọn chờ phần thưởng lớn hơn vì bạn tập trung hơn vào kế hoạch dài hạn và ít quan tâm đến sự thỏa mãn tức thì.

Hoạt động: Ưu tiên thời gian

Ưu tiên thời gian cao so với ưu tiên thời gian thấp

- 1 Hãy lắng nghe lời giải thích của giáo viên về lựa chọn kẹo.
- 2 Quyết định xem bạn muốn nhận một viên kẹo nhỏ hoặc một viên kẹo dẻo ngay bây giờ, hay đợi đến cuối lớp học để nhận hai viên kẹo hoặc một viên kẹo lớn hơn, hấp dẫn hơn.
- 3 Cam kết với quyết định của bạn và cho giáo viên biết lựa chọn đó. Nhận kẹo ngay lập tức hoặc vào cuối lớp học, tùy theo quyết định của bạn.
- 4 Tham gia thảo luận trên lớp về hoạt động, suy ngẫm về quá trình ra quyết định của bạn và khái niệm về ưu tiên thời gian.

Kết luận và thảo luận:

- 💡 Những yếu tố nào đã ảnh hưởng đến quyết định của bạn giữa việc nhận kẹo ngay bây giờ hay chờ đợi để nhận phần thưởng lớn hơn sau?
- 💡 Bạn cảm thấy thế nào về quyết định của mình khi hoạt động đã kết thúc?
- 💡 Bạn có thể nghĩ ra những ví dụ thực tế mà việc ưu tiên thời gian cao có thể gây hại và ưu tiên thời gian thấp có thể mang lại lợi ích không?
- 💡 Những hậu quả tiềm ẩn nào có thể xảy ra khi chọn ưu tiên thời gian cao thay vì ưu tiên thời gian thấp?

Trong bối cảnh của ví dụ về sa mạc, điều này có nghĩa là bạn có thể có xu hướng uống hết nước ngay lập tức, ngay cả khi điều đó có nghĩa là bạn sẽ không còn nước để dành cho sau này. Lý do là cơn khát bạn cảm thấy ngay lúc này cấp bách hơn cơn khát tiềm ẩn có thể xảy ra trong tương lai.

Mặt khác, nếu bạn chọn phân bổ nước và uống từ từ theo thời gian, bạn đang thể hiện ưu tiên thời gian thấp hơn. Điều này có nghĩa là bạn sẵn sàng chờ đợi để thỏa mãn cơn khát và nâng cao cơ hội sống sót của mình. Khái niệm chí phí cơ hội có liên quan chặt chẽ đến ý tưởng về sự khan hiếm và ưu tiên thời gian.

Tiền là gì?



Chi phí cơ hội đề cập đến giá trị của phương án thay thế tốt nhất tiếp theo mà bạn từ bỏ khi đưa ra quyết định. **Mọi quyết định đều liên quan đến sự đánh đổi.**

Lựa chọn hôm nay



Mua một ly sinh tố
dâu giá 7 đô la

Bây giờ



Chi 7 đô la theo cách khác

Sau này:



Hưởng lợi từ việc tiết kiệm
7 đô la đều đặn

Trong ví dụ về sa mạc, chi phí cơ hội của việc uống hết nước ngay lập tức chính là lợi ích sống còn mà bạn có thể nhận được nếu biết cách phân bổ nước và sử dụng nó trong một khoảng thời gian dài hơn.

Giả sử bạn quyết định phân bổ nước và uống từng ngụm nhỏ trong một khoảng thời gian dài hơn. Nhờ đó, bạn có đủ năng lượng và độ ẩm cần thiết để đi tìm thêm nước. Tuy nhiên, trong lúc tìm kiếm, bạn tình cờ gặp một cây xương rồng có một lượng nước nhỏ bên trong. Không nhiều, nhưng đủ để giải khát tạm thời. Nếu bạn đã uống hết toàn bộ nước chỉ trong một lần, có thể bạn sẽ không còn đủ năng lượng để đi tìm thêm nước và phát hiện ra cây xương rồng đó.

Trong trường hợp này, chi phí cơ hội của việc uống hết nước cùng một lúc chính là cơ hội tìm thấy cây xương rồng và có thêm nước để giải khát.

Ví dụ này minh họa rằng chi phí cơ hội không chỉ là sự đánh đổi ngay lập tức giữa hai lựa chọn, mà còn bao gồm cả những cơ hội tiềm năng trong tương lai có thể có được hoặc mất đi do quyết định của chúng ta.

Sự sẵn sàng từ bỏ phần thưởng lớn hơn trong tương lai để nhận phần thưởng nhỏ hơn ngay bây giờ của chúng ta chịu ảnh hưởng bởi ưu tiên thời gian, hay mức độ chúng ta đánh giá cao sự thỏa mãn tức thì so với kế hoạch dài hạn.

Trong chương này, chúng ta đã khám phá khái niệm cơ bản về tiền, bao gồm định nghĩa, chức năng, đặc điểm và các loại tiền khác nhau. Một phần quan trọng trong cuộc thảo luận là tìm hiểu tâm lý học về tiền, tập trung vào các khái niệm như sự khan hiếm, ưu tiên thời gian và chi phí cơ hội. Việc tìm hiểu này đã đặt nền tảng để hiểu rõ hơn về bản chất phức tạp của tiền và vai trò của nó trong cuộc sống của chúng ta. Trong chương tiếp theo, chúng ta sẽ tìm hiểu về lịch sử của tiền và cách mà nó đã phát triển theo thời gian.

Chương #3

Lịch sử của tiền

3.0 Giới thiệu

Hoạt động: Trò chơi đổi chác

3.1 Tiến hóa từ đổi chác đến tiền tệ hiện đại

3.1.1 Những vấn đề với các hình thức tiền sơ khai

3.1.2 Sự phát triển của tiền xu và tiền giấy

3.1.3 Chuyển đổi từ tiền vững chắc sang tiền không vững chắc

3.1.4 Từ giấy đến nhựa

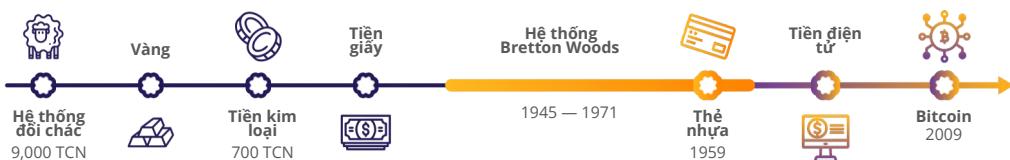
3.2 Tiền kỹ thuật số

Lịch sử của tiền

3.0 Giới thiệu

Tiền không được hình thành theo thiết kế, mà phát sinh từ quá trình thị trường. Nó không do chính phủ tạo ra, mà xuất hiện theo thời gian như một trật tự tự phát.

Murray Rothbard



Hãy tưởng tượng về một thời xa xưa khi con người không có tiền xu hay tiền giấy như chúng ta sử dụng ngày nay. Vào thời đó, họ có một cách giao dịch độc đáo — sử dụng các vật phẩm như vỏ sò hoặc kim loại quý như vàng như một loại tiền tệ đặc biệt. Điều này nghe có vẻ lạ, nhưng đó là dạng tiền tệ của họ, thứ mà mọi người đều đồng thuận là có giá trị. Trong chương này, chúng ta sẽ bắt đầu một hành trình xuyên thời gian, trực tiếp khám phá sự tiến hóa của tiền tệ. Chúng ta sẽ lần theo nguồn gốc của nó và quan sát cách nó thay đổi và thích nghi qua lịch sử.

Hoạt động: Bài tập trên lớp – Trò chơi đổi chác

Giáo viên sẽ phát cho bạn một mẫu giấy nhỏ. Mục tiêu của bạn là trao đổi món đồ bạn “có” để lấy món đồ bạn “mong muốn” trong một trò chơi mô phỏng hoạt động thương mại xuyên suốt lịch sử. Vui lòng ghi tên của bạn ở đầu tờ giấy bằng chữ nhỏ và dễ đọc.

Vòng #1: Đổi chác

Đó là năm 6000 TCN. Không cần nói cũng biết, tiền như chúng ta biết ngày nay vẫn chưa ra đời.

Bạn đang ở Mesopotamia và trực tiếp trao đổi hàng hóa và dịch vụ với nhau thông qua hình thức đổi chác.

Một lưu ý nữa là nhiều doanh nghiệp vẫn chấp nhận thanh toán không phải bằng tiền mặt cho các dịch vụ của họ và chính phủ coi các giao dịch đổi hàng này giống như các giao dịch tiền tệ cho mục đích báo cáo thuế.

Cắt tờ giấy theo đường đứt nét. Mục tiêu của bạn là trao đổi “có” của mình nhiều lần cần thiết để cuối cùng đạt được “mong muốn” ban đầu của bạn. Bạn không thể thay đổi “mong muốn” ban đầu của mình. Bạn sẽ có năm phút để hoàn thành mục tiêu của bài tập này.



Khi "có" mới của bạn khớp với "mong muốn" ban đầu, hãy quay lại chỗ ngồi. Sau khi hết thời gian, nếu bạn chưa tìm được đối tác trao đổi, hãy trở về chỗ ngồi dù sao đi nữa.



Hãy giơ tay nếu bạn đã trao đổi được món đồ mình muốn sau một lần trao đổi. Hai lần? Ba lần?

Trả lời ngắn gọn nhưng đầy đủ các câu hỏi sau:

1. Tại sao một số người có thể tìm được người để giao dịch trong khi những người khác thì không?

2. Những lợi ích của việc đổi chác là gì?

3. Dựa trên trải nghiệm của bạn với bài tập này, những hạn chế của việc đổi chác là gì?



Vòng #2: Tiền hàng hóa

Hãy tua nhanh đến bờ biển phía tây châu Phi vào khoảng thế kỷ 14 TCN. Việc đổi chác đã trở nên nhảm chán và không hiệu quả. Chúng ta đã phát triển thành một nền văn minh và hiện đang sử dụng **tiền hàng hóa**.

Từ vỏ ốc đến tiền xu



1300 TCN



1000 TCN



687 TCN



SỰ THẬT VUI VẺ

Vỏ ốc được chấp nhận làm phương tiện thanh toán hợp pháp ở một số vùng của châu Phi cho đến thế kỷ 20.

1300 TCN

Vỏ ốc là hình thức thanh toán chủ yếu ở hầu hết châu Á, châu Phi, châu Đại Dương và một số vùng của châu Âu.

1000 TCN

Triều đại Tây Chu của Trung Quốc bắt đầu sử dụng tiền kim loại.

687 TCN

Những đồng tiền nguyên thủy này có hình bầu dục, được làm từ "electrum" (hợp kim vàng và bạc), và chỉ có hoa văn ở một mặt.

Vua Alyattes của Lydia (nay thuộc Thổ Nhĩ Kỳ) ra lệnh đúc những đồng tiền kim loại đầu tiên ở thế giới phương Tây.

Lịch sử của tiền

Giáo viên đã đưa cho bạn một chiếc nui (hoặc một hình ảnh in của chiếc nui). Để đơn giản, ta giả sử giá của mỗi món hàng là một chiếc nui.

Mục tiêu của bạn vẫn là để có được những gì bạn “mong muốn,” nhưng giờ đây, loài người chúng ta đã thông minh hơn chút và tìm ra cách giải quyết một số vấn đề.

- 💡 Tại sao chúng ta lại coi nui là tiền hàng hóa?
 - 💡 Bây giờ chúng ta lấy được những thứ mình muốn bằng cách nào?
 - 💡 Vòng trao đổi sử dụng nui có dễ dàng hơn không?
 - 💡 Bạn nghĩ tại sao tiền lại thay thế cho hàng hóa?
 - 💡 Tiền hàng hóa hiệu quả hơn việc đổi chác ở những điểm nào?
 - 💡 Những hạn chế khi dùng nui làm tiền là gì?
 - 💡 Bạn nghĩ điều gì đã xảy ra khi Tây Ban Nha bắt đầu mang từng thuyền đầy nui trở về cộng đồng của bạn (ý chỉ vàng và bạc từ châu Mỹ)?
-
-
-
-

3.1 Tiến hóa từ đổi chác đến tiền tệ hiện đại

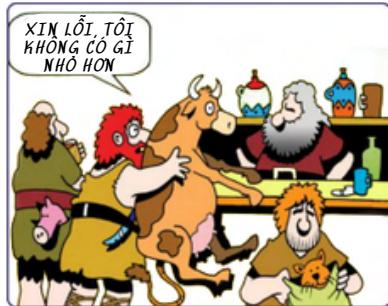
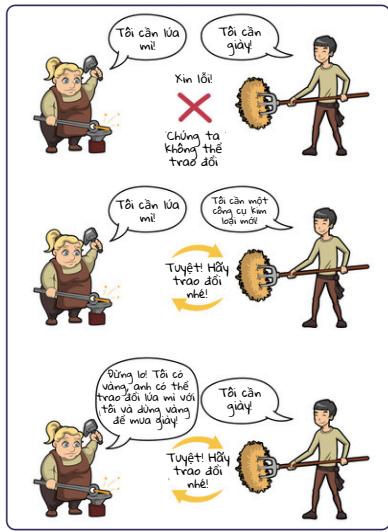
3.1.1 Những vấn đề với các hình thức tiền sơ khai



Xem video ngắn này để tìm hiểu về “Nguồn gốc của trao đổi” trong loạt phim “Lịch sử của tiền giấy.”

Trong các nền kinh tế đổi chác, con người giao dịch với nhau dựa trên giá trị tương đối của hàng hóa và dịch vụ mà họ sở hữu. Nền kinh tế đổi chác không hiệu quả và có thể khó quản lý, đặc biệt trong các xã hội phức tạp.

Một hiện tượng gọi là **trùng khớp nhu cầu** (double coincidence of want) là điều kiện cần thiết trong bất kỳ hệ thống đổi chác nào, vì người tham gia luôn phải tìm được người vừa có thứ họ cần, vừa cần đúng thứ họ đang có để trao đổi.



Giả sử:

- 👉 Joseph muốn đổi quả chuối của mình lấy quả dừa của Yael.
- 👉 Nhưng Yael chỉ muốn đổi quả dừa lấy quả xoài của Tammy.
- 👉 Còn Tammy thì chỉ muốn đổi quả xoài lấy quả chuối của Joseph.
- 👉 Họ bị kẹt trong một vòng luẩn quẩn của việc trao đổi trái cây mà không có sự trùng khớp nhu cầu.
- 👉 Joseph đề xuất rằng họ cứ đem trái cây đổi lấy một lon nước ngọt mát lạnh, nhưng rồi cả ba nhận ra họ đang ở trên một hòn đảo hoang, và chẳng có nước ngọt nào cả.
- 👉 Cuối cùng, họ quyết định ngồi trên bãi biển và yên lặng thưởng thức trái cây của mình.

Đây là tập thứ hai, có tựa đề "Không chỉ là mì", nằm trong loạt phim "Lịch sử của tiền giấy."



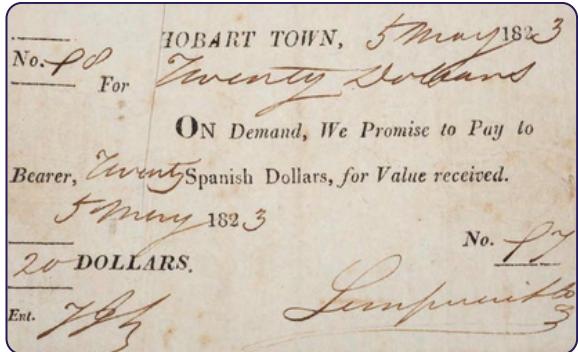
3.1.2 Sự phát triển của tiền xu và tiền giấy

Khi bạn và cộng đồng ngày càng tham gia nhiều hơn vào hoạt động thương mại, bạn nhận ra những hạn chế của việc đổi chác và các hình thức giao dịch không dùng tiền khác. Bạn quyết định sử dụng đồng tiền kim loại như một dạng tiền tệ.



Tiền hàng hóa là loại tiền được làm từ các kim loại quý như vàng và bạc. Trong lịch sử, chúng từng được sử dụng để cất trữ giá trị, làm phương tiện trao đổi, và trong quá khứ xa xôi còn là đơn vị hạch toán toán.

Lịch sử của tiền



và các kim loại quý khác và có thể quy đổi thành các kim loại này, như cách chúng từng được sử dụng từ thế kỷ 17 đến thế kỷ 19. Điều này cho phép bạn có một hình thức tiền tệ dễ mang theo và dễ trao đổi hơn trong khi vẫn duy trì được giá trị và tính an toàn của kim loại quý.



3.1.3 Chuyển đổi từ tiền vững chắc sang tiền không vững chắc

Bước nhanh đến thế kỷ 17 ở Thụy Điển. Lúc này, bạn hoàn toàn phụ thuộc vào các ngân hàng để lưu giữ tài sản quý giá của mình. Tuy nhiên, bạn bắt đầu nhận thấy có điều gì đó không ổn ở những người làm ngân hàng này; họ dường như đang phát hành nhiều giấy biên nhận hơn số vàng họ đang giữ trong kho, cho phép họ tạo ra nhiều tiền hơn so với tài sản thực tế đảm bảo. Thực tế lén lút này cho phép các ngân hàng kiếm lời từ khoản chênh lệch giữa giá trị của giấy biên nhận và giá trị vàng mà họ đang giữ cho khách hàng.

Chuyện gì sẽ xảy ra khi bạn thực sự cố gắng áp dụng nguyên tắc tiền giấy vào thực tế? Hãy tìm hiểu trong tập thứ tư của "Lịch sử Tiền Giấy."



Bạn nhận ra đây là một bước chuyển đổi quan trọng trong cách mà tiền tệ vận hành. Bạn đang chuyển từ một hệ thống tiền vững chắc (sound money, tức là tiền được bảo chứng bằng kim loại quý) sang một hệ thống tiền không vững chắc (unsound money, tức là tiền pháp định không được đảm bảo bằng tài sản vật chất). Quá trình chuyển đổi này không diễn ra trong một đêm, mà là một tiến trình từ từ chịu ảnh hưởng bởi nhiều yếu tố. Cuộc cách mạng công nghiệp, với sản xuất hàng loạt và đô thị hóa, đã đóng vai trò quan trọng, cũng như sự phát triển của các hệ thống tài chính tiên tiến như ngân hàng và thị trường chứng khoán. Sự xuất hiện của các ngân hàng trung ương và các cơ quan quản lý tiền tệ khác đã góp phần vào việc tập trung hóa và kiểm soát tiền tệ, dẫn đến việc phát hành tiền pháp định nhằm hỗ trợ tăng trưởng kinh tế.

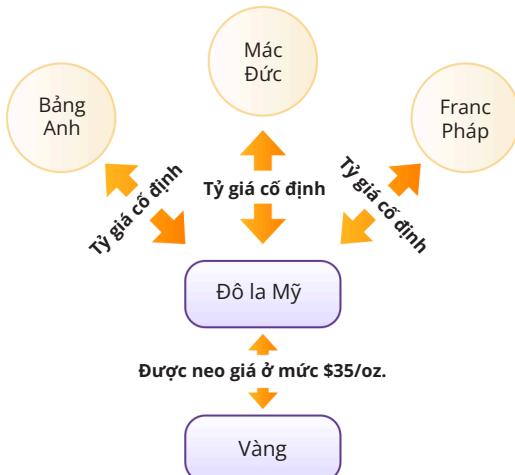


Tuy nhiên, bạn cũng bắt đầu nhận thấy **những mặt trái của sự tập trung hóa này**, bao gồm tiêu dùng thiếu trách nhiệm, **gia tăng nợ nần**, và việc thao túng người dân thông qua các biện pháp kích thích kinh tế.

Trước Chiến tranh Thế giới thứ nhất, bạn vẫn có thể quy đổi tiền giấy thành một lượng vàng cố định. Tuy nhiên, hai cuộc thế chiến cùng với cuộc khủng hoảng kinh tế năm 1929 đã chấm dứt điều đó. Năm 1944, Hiệp định Bretton Woods được ký kết, thiết lập đồng đô la Mỹ trở thành đồng tiền dự trữ của thế giới và cố định giá trị của đô la Mỹ theo giá vàng ở mức 35 đô la một ounce. Các đồng tiền của các quốc gia khác được neo giá theo đồng đô la, giúp ổn định các thị trường tài chính quốc tế.

Hệ thống Bretton Woods

(1945 — 1972)



Đáng tiếc là hệ thống này bắt đầu sụp đổ vào cuối những năm 1960, dẫn đến Cú sốc Nixon vào năm 1971, khi chính phủ Hoa Kỳ đình chỉ khả năng quy đổi đô la Mỹ ra vàng. Đây đánh dấu sự chấm dứt của bản vị vàng và sự khởi đầu của một thế giới vận hành dựa trên việc tạo ra và tích lũy nợ.

Trong cuộc sống hằng ngày, bạn bắt đầu nhận ra rằng giá trị của tiền tệ không còn ổn định như trước. Giống như một cây thước mềm khiến bạn khó đo chính xác chiều dài của một chiếc bàn, thì việc sống trong một thế giới tiền pháp định, nơi giá trị của tiền phụ thuộc vào sự biến động khó lường từ những người nắm quyền, cũng khiến bạn khó xác định chính xác giá trị của hàng hóa và dịch vụ. Bạn cảm thấy bối rối và bất an khi phải thích nghi với một thế giới mà giá trị của tiền không còn gắn với một tài sản vật chất như vàng nữa.

Lịch sử của tiền

Bạn thấy được những tác động của sự chuyển đổi này đến nền kinh tế toàn cầu và bắt đầu đặt câu hỏi về sự ổn định và đáng tin cậy của các loại tiền pháp định. Bạn nhận ra rằng, trong thế giới hiện đại, đồng đô la không còn được cố định và nhất quán như nó được neo giá theo vàng, mà thay vào đó phải chịu sự biến động. Điều này làm cho việc sử dụng đô la làm đơn vị hạch toán trở nên khó khăn hơn, vì giá trị của nó bị ảnh hưởng bởi nhiều yếu tố như lạm phát (giá cả tăng), lãi suất, sức mạnh kinh tế của quốc gia, các sự kiện chính trị, đầu cơ thị trường, và nhu cầu trong thương mại quốc tế. Đây là khoảng thời gian đầy bối rối và khó đoán khi bạn cố gắng điều hướng giá trị đô la luôn thay đổi và tác động của nó đến cuộc sống hàng ngày của bạn.

Mặc dù đã có những nỗ lực cải thiện chất lượng cuộc sống thông qua hệ thống tiền tệ hiện đại, nâng cao hiệu quả, mở rộng tiếp cận thông tin và cải thiện giao tiếp, nhưng phần lớn mức sống của người dân bắt đầu suy giảm do:

- ◆ Lạm dụng quyền lực tập trung
- ◆ Giá cả tăng cao
- ◆ Tiền lương thực tế bị đình trệ
- ◆ Tiền tệ yếu đi
- ◆ Cần chi tiêu nhiều tiền hơn để mua được ít thứ hơn

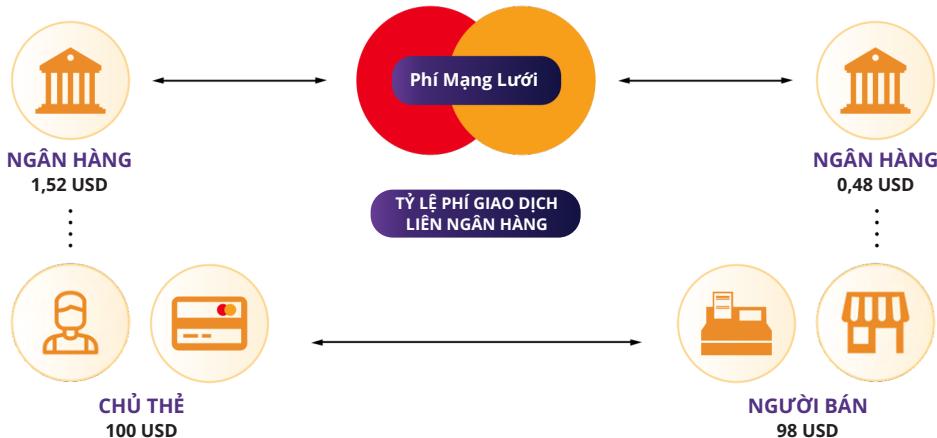
Điều này tạo ra những thách thức cho những người có nguồn lực kinh tế hạn chế, khi họ có thể bị hạn chế trong việc tiếp cận giáo dục, tín dụng, nguồn lực, mạng lưới xã hội và đại diện chính trị, dẫn đến những bất lợi tiềm tàng trong khả năng thành công của họ.

Kết quả là người giàu có dường như càng ngày càng giàu hơn, trong khi người nghèo lại càng ngày càng nghèo đi.



3.1.4 Từ giấy đến nhựa

Ngày nay, chúng ta đã đi một chặng đường dài kể từ khi thẻ tín dụng đầu tiên được ra đời vào những năm 1950. Chỉ với một cái vuốt nhẹ trên tấm nhựa, chúng ta có thể mua bất cứ thứ gì mình muốn, bất cứ lúc nào mà không gặp phải khó khăn nào. Nó giống như mở ra một thế giới đầy những khả năng vô tận, và sự háo hức khám phá những điều mới mẻ đó thật sự rất rõ ràng... hoặc ít nhất thì chúng ta đã từng nghĩ vậy. Ít ai biết rằng sự phụ thuộc vào tín dụng lại mang đến những hệ quả đau đớn — như làm tăng tổng chi phí hàng hóa và khuyến khích một nền kinh tế có nguy cơ thất bại.



Khi công nghệ phát triển, cách chúng ta quản lý tiền cũng thay đổi theo. Internet đã trở thành một yếu tố quan trọng trong thế giới tài chính, với ngân hàng trực tuyến và các trang thương mại điện tử cho phép chúng ta quản lý và chi tiêu tiền hoàn toàn trên mạng.

Sự phát triển của tiền kỹ thuật số đánh dấu bước tiến quan trọng tiếp theo trong quá trình này, mở ra những khả năng mới và định hình lại cách chúng ta thực hiện các giao dịch tài chính.

3.2 Tiền kỹ thuật số

Không giống như các loại tiền truyền thống, tiền kỹ thuật số chỉ tồn tại dưới dạng điện tử. Chúng được lưu trữ và giao dịch thông qua máy tính và phần mềm chuyên dụng.

Tiền kỹ thuật số cho phép mọi người gửi tiền qua internet. Giống như email cho phép chúng ta gửi tin nhắn tức thì mà không cần chi phí vận chuyển, tiền kỹ thuật số cũng cho phép chúng ta chuyển và nhận giá trị một cách gần như tức thời và với chi phí rất thấp.

Ngày nay, các loại tiền tệ mà chúng ta đang sử dụng ngày càng mang tính kỹ thuật số. Chỉ một phần rất nhỏ của tổng cung tiền tồn tại dưới dạng tiền xu và tiền giấy. Các ngân hàng và dịch vụ tài chính cung cấp ứng dụng cho người dùng để dễ dàng chuyển tiền qua mạng. Nhưng tiền thực sự đến từ đâu?

Trong chương này, chúng ta đã chứng kiến quá trình chuyển đổi từ tiền vững chắc, được đại diện bởi vàng, sang tiền không vững chắc dưới dạng giấy, và giờ là tiền pháp định kỹ thuật số. Ở chương tiếp theo, chúng ta sẽ tìm hiểu cách hệ thống tiền pháp định hiện tại vận hành và nguồn gốc hình thành của nó.

Chương #4

Tiền pháp định là gì và ai kiểm soát nó?

4.0 Giới thiệu

4.1 Lược sử về tiền pháp định

4.2 Hệ thống tiền pháp định

4.2.1 Hệ thống tiền tệ theo nghị định

4.2.2 Ngân hàng dự trữ một phần: hệ thống được thúc đẩy bởi nợ

Hoạt động: Ngân hàng dự trữ một phần

4.2.3 Ai kiểm soát hệ thống tiền pháp định và họ hưởng lợi ra sao?

4.3 Tiền tệ kỹ thuật số của ngân hàng trung ương: Tương lai của tiền pháp định

Tiền pháp định là gì và ai kiểm soát nó?

4.0 Giới thiệu

Lịch sử nhân loại là lịch sử của đồng tiền mất giá.

Milton Friedman

Chúng ta đã thấy trong chương trước cách mà tiền tệ đã phát triển theo thời gian và cách hệ thống tiền tệ của chúng ta chuyển đổi từ tiền vững chắc sang tiền không vững chắc, qua đó hình thành nên thế giới mà chúng ta đang sống ngày nay. Chương này sẽ đi sâu hơn vào cách những thay đổi đó dẫn đến hệ thống tiền pháp định hiện tại và cách mà hệ thống này vận hành.

Vậy, hệ thống tiền pháp định này trông như thế nào, và nó đã ra đời như thế nào?

Để trả lời câu hỏi này, trước tiên chúng ta cần tập trung vào đồng đô la Mỹ, đồng tiền dự trữ của thế giới hiện nay, vốn đóng vai trò thống trị trong thế giới ngày nay. Mỗi quốc gia, dù trực tiếp hay gián tiếp, đều chịu ảnh hưởng từ các quyết định liên quan đến đồng đô la Mỹ. Để thực sự hiểu cách mà hệ thống tiền pháp định vận hành tại quốc gia của bạn, điều thiết yếu là phải lần theo các mốc lịch sử kết nối nó với nơi khởi nguồn của hệ thống tiền pháp định — Hợp chủng quốc Hoa Kỳ.

4.1 Lược sử về tiền pháp định

1815-1933	1913	1933	1934	1944	1971	1980
Tiêu chuẩn vàng	Thành lập Ngân hàng Trung ương có tên là "The Federal Reserve"(Cục Dự trữ Liên bang Hoa Kỳ)	Sắc lệnh hành pháp 6102. Mọi công dân buộc phải giao nộp vàng với tỷ giá 20,67 đô la mỗi ounce vàng	Đạo luật Dự trữ Vàng. Cướp đoạt tài sản của người dân bằng cách phá giá đồng đô la 40%, đưa giá vàng lên 35 đô la mỗi ounce	Thỏa thuận Bretton Woods: USD trở thành đồng tiền dự trữ thống trị của thế giới	Cú sốc Nixon, sự kiện đánh dấu sự ra đời của hệ thống tiền pháp định bằng cách chấm dứt khả năng quy đổi đồng đô la Mỹ ra vàng	Giá vàng tăng từ 35 đô la mỗi ounce vào năm 1970 lên 870 đô la mỗi ounce vào năm 1980, khiến đồng tiền của người dân mất 96% giá trị chỉ trong vòng 10 năm

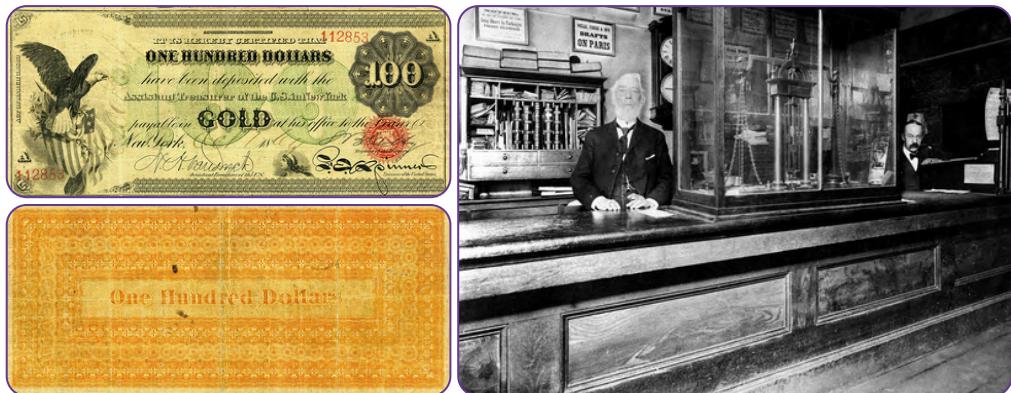
Sơ đồ dòng thời gian

Vào thế kỷ 19, các nền văn minh trên khắp thế giới phát triển thịnh vượng nhờ sử dụng tiền vững chắc, đó là các kim loại quý như vàng và bạc, vốn nổi bật với tính khan hiếm, tính lâu bền và khả năng nhận biết cao. Khi thương mại toàn cầu mở rộng, việc mang theo số lượng lớn kim loại trở nên bất tiện, dẫn đến sự ra đời của các kho lưu trữ vàng và bạc. Những kho này bảo quản an toàn tài sản quý giá của người dân và cung cấp các giấy chứng nhận có thể quy đổi thành một lượng vàng hoặc bạc cụ thể. Đổi lại việc gửi tiền, người dân nhận được giấy chứng nhận gắn liền trực tiếp với đúng



Chương #4

số vàng hoặc bạc mà họ đã gửi. Mỗi liên kết trực tiếp giữa giấy chứng nhận và tiền hàng hóa hữu hình này đánh dấu giai đoạn đầu của những gì ngày nay chúng ta gọi là ngân hàng.



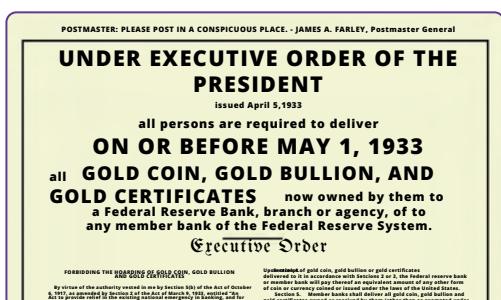
Ban đầu, các ngân hàng nhằm bảo vệ tiền của khách hàng nhưng sau đó bắt đầu tham gia vào các hoạt động cho vay rủi ro, phát hành giấy chứng nhận cho lượng vàng vượt quá số vàng họ thực sự sở hữu. Việc này dẫn đến nguy cơ rút tiền hàng loạt nếu quá nhiều khách hàng cùng lúc yêu cầu nhận lại tiền của mình. Để đối phó



với rủi ro này, các ngân hàng đã hợp tác với chính phủ để thiết lập một hệ thống hợp pháp hóa việc cho vay lại. Năm 1913, họ thành lập Cục Dự trữ Liên bang, một ngân hàng trung ương chịu trách nhiệm phát hành các giấy chứng nhận mới và cung cấp các ngân hàng gấp khó khăn. Trên toàn cầu, các chính phủ nhận thức được giá trị của vàng và bạc, dẫn đến các cuộc xung đột và chiến tranh nhằm giành quyền kiểm soát. Trong những năm dẫn đến Thế chiến II, các lãnh đạo như Lenin, Stalin, Churchill, Roosevelt, Mussolini và Hitler đã tịch thu vàng vì các mục đích chiến lược.

Vào đầu những năm 1930, một thay đổi quan trọng đã diễn ra trong cách tiền tệ được bảo chứng bằng tài sản tại Hoa Kỳ. Vào thời điểm đó, phần lớn tài sản của người dân được giữ dưới dạng vàng. Tuy nhiên, năm 1933, Tổng thống Roosevelt đã ban hành Sắc lệnh hành pháp 6102, yêu cầu mọi công dân phải giao nộp vàng của mình. Đây không phải là một việc trao đổi tự nguyện — người dân bắt buộc phải giao nộp vàng, và nếu từ chối, họ sẽ phải đối mặt với các hình phạt nghiêm trọng.

Chính phủ đã ấn định tỷ giá là 20,67 đô la cho mỗi ounce vàng. Điều này có nghĩa là mỗi ounce vàng mà một người sở hữu sẽ được đổi lấy giấy chứng nhận giấy trị giá tương đương 20,67 đô la. Người dân buộc phải chấp nhận các đồng đô la giấy này với hy vọng một ngày nào đó có thể đổi lại vàng.

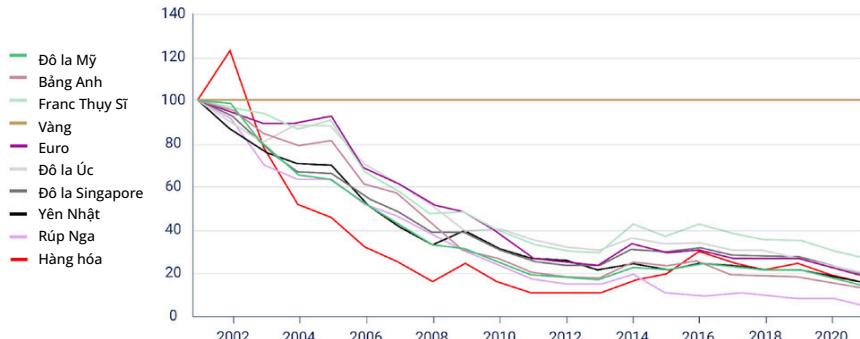


Tiền pháp định là gì và ai kiểm soát nó?

Năm 1934, Đạo luật Dự trữ Vàng cho phép người dân được đổi lại đô la giấy lấy vàng. Tuy nhiên, có một điểm bất lợi: chính phủ cố tình làm mất giá đô la giấy bằng cách tăng tỷ giá trao đổi lên 35 đô la cho mỗi ounce vàng. Việc phá giá này đã ảnh hưởng nặng nề đến những người lao động thuộc tầng lớp trung lưu và thấp, vì khoản tiết kiệm của họ trước đây có giá trị cao hơn nay trở nên kém giá trị do sức mua của đô la giấy giảm.

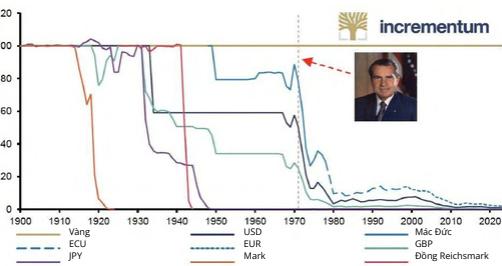
Sau Thế chiến II, Thỏa thuận Bretton Woods vào năm 1944 quy định rằng đồng đô la Mỹ sẽ trở thành đồng tiền dự trữ của thế giới và có thể được quy đổi ra vàng. Tuy nhiên, mối liên kết giữa đô la Mỹ và vàng đã bị cắt đứt vào năm 1971 khi Tổng thống Nixon chấm dứt khả năng quy đổi đô la Mỹ lấy vàng. Đây là một bước ngoặt quan trọng, đánh dấu sự chuyển đổi sang hệ thống tiền pháp định, nơi giá trị của đồng tiền không còn được bảo chứng bằng một loại hàng hóa vật chất như vàng, mà dựa trên niềm tin và sự tín nhiệm của người sử dụng. Khi các chính phủ và ngân hàng trung ương giữ lại phần lớn lượng vàng của người dân, giá trị của vàng tăng mạnh, đạt 870 đô la mỗi ounce vào năm 1980.

Giá trị theo ounce của USD/vàng



Tóm lại, câu chuyện về việc xã hội loài người chuyển từ tiêu chuẩn tiền vững chắc sang tiêu chuẩn tiền không vững chắc (tiền pháp định) cho thấy cách mà chính phủ và ngân hàng đã chiếm đoạt các kim loại quý từ người dân. Trong khi tiền thật rơi vào tay chính phủ và ngân hàng, người dân chỉ còn lại những mảnh giấy mà giá trị duy nhất đến từ việc chính phủ bắt buộc phải sử dụng.

Vàng và các loại tiền tệ đo lường theo vàng, 1900-2023



Nguồn: World Gold Council, Reuters Elkon, incrementum AG

4.2 Hệ thống tiền pháp định

Vấn đề cốt lõi của tiền tệ truyền thống là sự tin tưởng tuyệt đối mà nó đòi hỏi để vận hành. Ngân hàng trung ương phải được tin tưởng không làm mất giá đồng tiền, nhưng lịch sử của các loại tiền pháp định lại đầy rẫy những sự phá vỡ niềm tin đó.

Satoshi Nakamoto

Loài người đã chuyển từ tiền vững chắc do nhiều người kiểm soát sang tiền không vững chắc do một số ít kiểm soát. Nhưng hệ thống này hoạt động chính xác như thế nào?

4.2.1 Hệ thống tiền tệ theo nghị định

Hệ thống tiền pháp định được đặc trưng bởi tính bắt buộc, áp đặt lên người dân qua các luật bắt buộc sử dụng tiền. Thuật ngữ "fiat," (tiền pháp định) có nguồn gốc từ tiếng Latin, nghĩa là "theo sắc lệnh," thể hiện chỉ thị do nhà chức trách ban hành.

Không giống như tiền được bảo chứng bằng tài sản hữu hình như vàng, tiền pháp định không có sự hỗ trợ đó. Thay vào đó, việc sử dụng tiền pháp định được pháp luật quy định bắt buộc. Các đồng tiền hàng ngày như đô la, euro, bảng Anh, nhân dân tệ, peso và nhiều loại khác đều thuộc loại tiền pháp định.

Luật tiền pháp định: Luật quy định bắt buộc tất cả công dân phải chấp nhận một loại tiền tệ nhất định.



Giá trị của tiền pháp định dựa trên niềm tin rằng nó có thể được dùng để trao đổi hàng hóa và dịch vụ, cùng với ảo tưởng rằng nó sẽ giữ được giá trị theo thời gian. Tiền pháp định giống như một tấm vé hòa nhạc; giá trị không nằm ở tờ vé giấy mà ở sự đảm bảo rằng ban nhạc (chính phủ và ngân hàng trung ương) sẽ mang đến một buổi biểu diễn tuyệt vời (đảm bảo ổn định kinh tế).

Ưu điểm của tiền pháp định

- ◆ **Dễ sử dụng:** Tiền pháp định tiện lợi cho các giao dịch hàng ngày.
- ◆ **Chi phí và rủi ro thấp hơn:** Tiền pháp định không yêu cầu bảo mật cao như vàng, khiến nó rẻ hơn và an toàn hơn.

Nhược điểm của tiền pháp định

- ◆ **Rủi ro lạm phát:** Giá cả có thể tăng liên tục, gây ra lạm phát và trong lịch sử đã từng xảy ra siêu lạm phát.
- ◆ **Kiểm soát tập trung và thao túng:** Một nhóm nhỏ có thể ảnh hưởng và thao túng hệ thống, dẫn đến kiểm duyệt và tịch thu tài sản.
- ◆ **Rủi ro đối tác:** Nếu chính phủ gặp khó khăn, đồng tiền có thể mất giá trị.
- ◆ **Tiềm ẩn lạm dụng:** Hệ thống có thể bị lợi dụng, dẫn đến tham nhũng và mất niềm tin.

Tiền pháp định là gì và ai kiểm soát nó?

Tiền hàng hóa và tiền pháp định: Hình dung sự khác biệt

Hãy nhớ rằng: Trước khi tiền pháp định xuất hiện, các chính phủ đúc tiền bằng các loại hàng hóa vật chất có giá trị, khan hiếm và khó khai thác như vàng hoặc bạc, hoặc in tiền giấy có thể quy đổi thành một lượng nhất định hàng hóa vật chất đó. Đây là hệ thống tiền được bảo chứng bằng hàng hóa.

Còn trong hệ thống tiền pháp định, nó giống như tiền trong trò chơi Cờ tỷ phú. Tiền trong hệ thống này là những tờ giấy do ngân hàng trung ương in ra, và giá trị của nó chịu ảnh hưởng trực tiếp từ chính sách của chính phủ. Chính phủ và ngân hàng trung ương giống như “những người chơi ngân hàng trong trò chơi Cờ tỷ phú,” kiểm soát cách thức trò chơi vận hành, ai nhận được gì, và giá trị của từng đồng tiền. Nói cách khác, chính phủ cam kết quản lý hệ thống tiền tệ một cách hiệu quả.

Tóm lại, tiền pháp định chỉ có giá trị khi chính phủ ra lệnh sử dụng; bản thân tiền pháp định không có tiện ích riêng.

Đúc kết lại, hệ thống tiền pháp định là một trò chơi dựa trên niềm tin, nơi giá trị của đồng tiền phụ thuộc vào những lời hứa của những người có quyền lực, và người dân chỉ có thể hy vọng chính phủ sẽ hành động vì lợi ích chung. Tiếp theo, chúng ta sẽ tìm hiểu cách các ngân hàng tạo ra tiền mới, những ai tham gia, và điều đó ảnh hưởng như thế nào đến nền kinh tế.

4.2.2 Ngân hàng dự trữ một phần: hệ thống được thúc đẩy bởi nợ

Thật may mắn là người dân trong nước không hiểu hệ thống ngân hàng và tiền tệ của chúng ta, vì nếu hiểu, tôi tin rằng sẽ có một cuộc cách mạng ngay trước sáng mai.

Henry Ford

Ngân hàng dự trữ phân đoạn là một trong những thành phần chính của hệ thống tiền pháp định, cho phép các ngân hàng cho vay phần lớn tiền gửi của khách hàng. Bạn đã bao giờ tự hỏi tại sao các ngân hàng lãi cung cấp nhiều dịch vụ đến vậy? Dù có vẻ như họ rất hào phóng, nhưng bạn cần nhớ rằng ngân hàng là doanh nghiệp và mục tiêu chính của họ là kiếm lời. Vậy họ kiếm lời bằng cách nào nếu cho người ta vay tiền?

Ngoài việc kiếm lãi từ tiền gửi, các ngân hàng còn tạo ra doanh thu bằng nhiều cách khác, bao gồm:

- ☀ Tính lãi trên các khoản vay mà họ cho khách hàng
- ☀ Thu phí dịch vụ như sử dụng máy ATM và duy trì tài khoản
- ☀ Kiếm tiền từ đầu tư, ví dụ mua bán chứng khoán hoặc đầu tư bất động sản
- ☀ Giữ một tỷ lệ phần trăm khoản vay trong dự trữ và đầu tư hoặc cho vay phần còn lại
- ☀ Trả lãi cho tiền gửi và thu phí từ các tài khoản thanh toán và tiết kiệm

Khi ngân hàng nhận tiền gửi, họ chỉ cần giữ một phần nhỏ (dự trữ bắt buộc) và có thể cho vay phần còn lại.



Các ngân hàng vay tiền từ người gửi với lãi suất
(giả sử là 5%)

Ngân hàng cho vay số tiền này cho người đi vay với mức lãi suất cao hơn.
(giả sử là 9%)



Ngân hàng trả lãi cho người gửi từ số lãi nhận được khi cho vay
(9% - 5% = 4%) và giữ phần còn lại làm lợi nhuận

Ví dụ, nếu bạn gửi 100 đô la với tỷ lệ dự trữ bắt buộc là 10%, ngân hàng chỉ cần giữ lại 10 đô la làm dự trữ và có thể cho vay 90 đô la. Người đi vay sau đó gửi 90 đô la này vào một ngân hàng khác, khiến chu trình tiếp tục diễn ra. Mặc dù ban đầu chỉ có 100 đô la được gửi, tổng lượng tiền trong nền kinh tế có thể tăng lên tới 271 đô la, dường như xuất hiện từ hư không — hiện tượng này được gọi là hiệu ứng nhân.

Quá trình này dẫn đến một hệ thống tiền tệ dựa trên nợ khi các ngân hàng tạo ra tiền mới mỗi khi cho vay, làm tăng tổng cung tiền trong nền kinh tế. Khi hệ thống ngân hàng dự trữ bắt buộc tiếp tục hoạt động, tổng nợ trong nền kinh tế tăng lên, góp phần gây ra lạm phát.

Hệ thống dựa vào một vòng tuần hoàn liên tục của việc tạo ra tiền thông qua cho vay, giống như việc cung cấp thuốc đều đặn cho người nghiện. Tuy nhiên, nếu ngân hàng cho vay nhiều hơn số tiền dự trữ và đồng thời nhiều người gửi tiền đồng loạt rút, ngân hàng có thể bị phá sản.

Tại đây, ngân hàng trung ương can thiệp với vai trò là người cho vay cuối cùng, cung cấp tiền tệ mới nhằm ngăn chặn sự sụp đổ của các ngân hàng. Ngân hàng trung ương thực hiện điều này bằng cách mua lại tài sản hoặc bơm trực tiếp tiền tệ vào tài khoản của các ngân hàng. Về bản chất, các ngân hàng được cứu khỏi phá sản nhờ vào việc liên tục bơm tiền mới từ ngân hàng trung ương. Hệ thống dựa trên nợ và liên tục được cứu trợ bởi ngân hàng trung ương này dẫn đến các chu kỳ bùng nổ và suy thoái.

Hãy tưởng tượng bạn có một người bạn làm nghề ngân hàng; ta hãy gọi anh ấy là Dax.

Dax rất thích xe đẹp, và anh ấy muốn mượn chiếc xe của bạn vì có nhiều nơi cần đi. Bạn cho anh ấy mượn xe, nhưng rồi có một điều bất ngờ: Dax bắt đầu hứa sẽ cho nhiều người bạn khác mượn cùng một chiếc xe đó. Từ một chiếc xe thật mà bạn đã cho anh ấy mượn, Dax tạo ra những chiếc xe “tưởng tượng” và bắt đầu cho bạn bè mượn. Mỗi người đều nghĩ rằng họ có thể thoải mái đạp xe khi nào mình muốn. Nhưng đây là điều bất ngờ — chỉ có một chiếc xe thật! Còn lại đều là xe tưởng tượng, chỉ là những lời hứa.

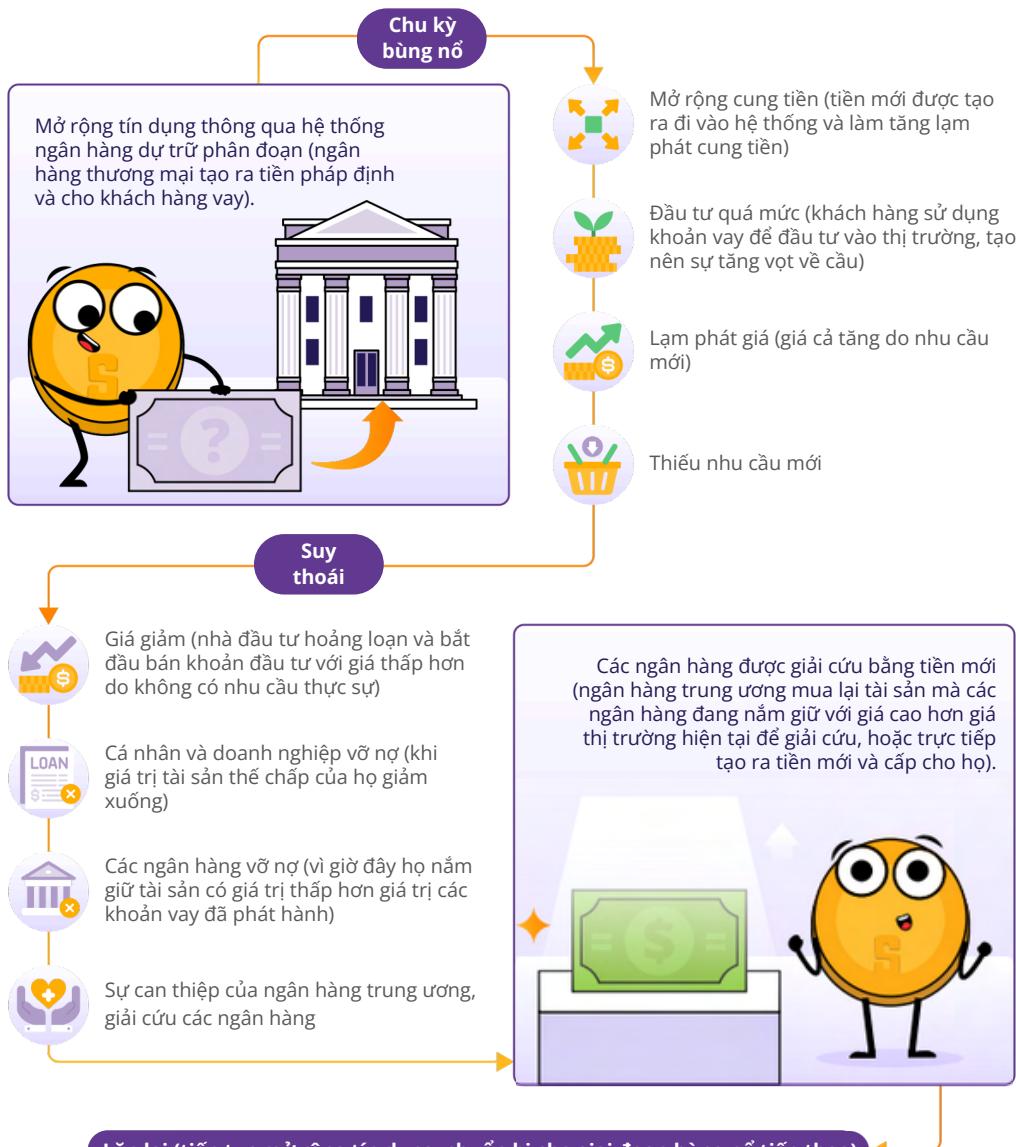
Vậy chuyện gì xảy ra? Khi càng nhiều chiếc xe đẹp “tưởng tượng” được cho mượn, mọi người đều rất vui, ít nhất là lúc đầu, vì không ai sử dụng xe cùng một lúc — mọi thứ trông có vẻ ổn; ai cũng cảm thấy như có rất nhiều xe cho tất cả mọi người. Thế là tất cả bạn bè bắt đầu lên thêm nhiều kế hoạch, nghĩ về những nơi họ sẽ đến với chiếc xe của mình.

Tuy nhiên, đây chính là lúc phép màu bắt đầu mất đi sự hấp dẫn. Một ngày nắng đẹp, mọi người đều quyết định rằng hôm nay là ngày lý tưởng để đi đạp xe. Họ cùng nhau đến trước cửa nhà Dax, háo hức muốn thử những chiếc xe tưởng tượng của mình. Nhưng rồi, thực tế ập đến — chỉ có một chiếc xe thật. Sự thất vọng lan tỏa, và giá trị của những chuyến đi hứa hẹn bỗng chốc giảm sút.

Trong thế giới cho vay dự trữ phân đoạn, câu chuyện cũng tương tự. Các ngân hàng cho vay nhiều tiền hơn số tiền thực tế họ có, và trong một thời gian, mọi người đều hưởng lợi. Tiền được lưu thông nhiều hơn, và dường như có đủ cho tất cả. Nhưng nếu quá nhiều người cùng rút tiền một lúc, giá trị thực sự sẽ lộ rõ: không đủ tiền để đáp ứng tất cả các cam kết.

Tình huống này ảnh hưởng đến lợi ích chung và giá trị của tất cả mọi người liên quan. Lời hứa về sự thịnh vượng biến thành một trò lừa đảo. Cũng giống như những chiếc xe đẹp tưởng tượng mất đi giá trị trong mắt mọi người khi ai cũng muốn có một chuyến đi thật, giá trị của tiền trong nền kinh tế cũng có thể giảm sút khi mọi người đổ xô đòi lấy phần thực của mình. Khi điều đó xảy ra, mọi người nhận ra rằng số tiền họ gửi trong ngân hàng thực ra không có thật, dẫn đến hoảng loạn, chạy ngân hàng và thậm chí là sự sụp đổ của cả nền kinh tế. Những người phải gánh chịu hậu quả của những sự sụp đổ này, cho đến nay, luôn là cùng một nhóm: tầng lớp trung lưu và thấp hơn trên toàn thế giới.

Tiền pháp định là gì và ai kiểm soát nó?



Hoạt động: Ngân hàng dự trữ một phần

Trong bài tập sau đây, chúng ta sẽ khám phá cách hệ thống ngân hàng dự trữ một phần có thể dẫn đến làm mất giá tiền tệ, lạm phát và suy giảm sức mua. Chúng ta sẽ sử dụng một ví dụ đơn giản với sáu người tham gia, trong đó một người đóng vai trò là ngân hàng, với tỷ lệ dự trữ vẫn còn được sử dụng phổ biến cho đến ngày nay: 10%.

- ✿ Người A vừa trúng xổ số 100.000 đô la và gửi số tiền này vào ngân hàng (B). Với tỷ lệ dự trữ 10%, ngân hàng B phải giữ lại 10.000 đô la trong két, và có thể cho vay 90.000 đô la còn lại.
- ✿ Người C vay số tiền tối đa (90.000 đô la) từ B và dùng số tiền đó để mua nhà từ D.
- ✿ Người D gửi 90.000 đô la nhận được từ người C vào ngân hàng (B). Tổng số tiền gửi trong ngân hàng hiện là 190.000 đô la.
- ✿ Người E vay tiền từ ngân hàng B, và ngân hàng cho vay 90% số tiền gửi mới, tức là 81.000 đô la.
- ✿ Người E dùng khoản vay 81.000 đô la để mua một tác phẩm nghệ thuật từ người F, người này sau đó gửi số tiền vào ngân hàng (B). Tổng số tiền gửi được ghi nhận hiện là 271.000 đô la.

Trong trường hợp này, khoản tiền gửi ban đầu 100.000 đô la đã tạo ra tổng số 271.000 đô la tiền gửi sau khi lưu thông trong nền kinh tế.

Nếu tỷ lệ dự trữ giảm xuống còn 1%, lượng tiền được tạo ra sẽ tăng đáng kể ($100.000 \text{ đô la} / 0,01 = 10.000.000 \text{ đô la}$). Trong trường hợp này, với 100.000 đô la đó, thực tế sẽ tạo ra bao nhiêu tiền nếu tiền tiếp tục lưu thông trong nền kinh tế?

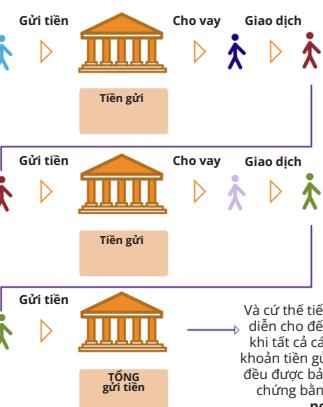
Cần lưu ý rằng kể từ năm 2020, Cục Dự trữ Liên bang Mỹ (Ngân hàng Trung ương Hoa Kỳ) đã giảm tỷ lệ dự trữ bắt buộc xuống còn 0% nhằm kích thích nền kinh tế.

Chúng ta cần các tinh nguyên viên sau:

- A** = Người gửi tiền (Người trúng xổ số) (Xanh da trời nhạt)
- B** = Thu ngân ngân hàng (Ngân hàng)
- C** = Con nợ số 1 (Xanh dương đậm)
- D** = Chủ sở hữu tài sản / Người gửi tiền (Đỏ)
- E** = Con nợ số 2 (Tím nhạt)
- F** = Chủ phòng tranh / Người gửi tiền (Xanh lá cây)

Ngân hàng dự trữ một phần

Giữ lại 1/2



Tiền pháp định là gì và ai kiểm soát nó?

4.2.3 Ai kiểm soát hệ thống tiền pháp định và họ hưởng lợi ra sao?

Có bốn bên chính: chính phủ, các cá nhân giàu có, khu vực tài chính và ngân hàng trung ương. Họ cùng nhau kiểm soát hệ thống tiền pháp định.

Chính phủ: Chính phủ giống như đạo diễn của vở kịch tiền pháp định. Ngoài việc thu thuế, họ còn được tài trợ thông qua các khoản nợ mới (trái phiếu) do Bộ Tài chính phát hành. Khi nhu cầu mua các trái phiếu này không đủ, phần nợ còn lại sẽ được ngân hàng trung ương mua vào. Điều này cho phép chính phủ tiếp tục các hoạt động và theo đuổi lợi ích của mình mà không cần sự chấp thuận từ người dân. Nó giống như việc có một thẻ tín dụng mà không phải lo trả nợ ngay. Nghe có vẻ có lợi cho chính phủ, nhưng cái giá phải trả lại đỗ lén vai tất cả mọi người.

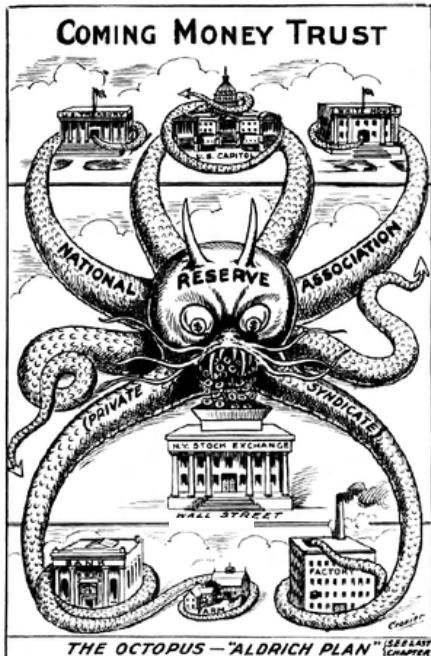
Cá nhân giàu có: Những cá nhân giàu có được hưởng lợi rất nhiều từ hệ thống tiền pháp định. Với khả năng vay nợ ngày càng nhiều, họ có thể đầu tư vào các tài sản như hàng hóa, bất động sản và cổ phiếu, từ đó tạo ra của cải mới gần như không tổn công sức.

Khu vực tài chính (ngân hàng): Các ngân hàng và tổ chức tài chính khác không trực tiếp kiểm soát hệ thống tiền pháp định nhưng lại hưởng lợi rất nhiều từ nó. Không bị ràng buộc bởi trách nhiệm giải trình, họ có thể thúc đẩy việc tạo ra tiền tệ mới thông qua hoạt động cho vay dự trữ một phần, từ đó thu được lợi nhuận cao hơn. Các ngân hàng hầu như không phải chịu hậu quả vì thường được giải cứu bằng tiền pháp định mới nhằm ngăn chặn sự sụp đổ của toàn bộ hệ thống.

Ngân hàng trung ương: Ngân hàng trung ương là kẻ giật dây, được cho là kiểm soát tốc độ tăng trưởng của nguồn cung tiền. Nhưng có một điều đáng nói — ngân hàng trung ương cũng chịu sự chi phối bởi luật pháp của chính phủ và phục vụ cho lợi ích của chính phủ. Nó giống như một người điều khiển rối lại bị một người điều khiển khác kiểm soát. Ngân hàng trung ương có thể trông như đang nắm quyền, nhưng thực chất đang gián tiếp thực hiện mong muốn của chính phủ: in tiền từ con số không khi họ cần.

Cách họ hưởng lợi: Những nhóm này hưởng lợi theo nhiều cách khác nhau, tạo nên một mạng lưới kiểm soát phức tạp. Chính phủ có được nguồn vốn mà không phải gánh chịu hậu quả ngay lập tức, các cá nhân giàu có và ngân hàng thì kiếm tiền một cách dễ dàng, còn ngân hàng trung ương giữ cho hệ thống tiếp tục vận hành. Trong khi đó, phần còn lại của người dân có thể sẽ cảm nhận được tác động, phải đổi mới với nhiều khó khăn khi hệ thống này vận hành.

Cuối cùng, những kẻ giật dây trong hệ thống tiền pháp định tạo ra một màn trình diễn mà trong đó một số ít người hưởng lợi rất nhiều, còn phần đông lại tự hỏi về sự công bằng của sân khấu tài chính mà họ đang đứng trên đó.



Vai trò của ngân hàng trung ương

Ngân hàng trung ương âm thầm định hình cách một nền kinh tế vận hành. Nhiệm vụ chính thức của họ là đảm bảo sự ổn định, tính toàn vẹn và "giữ cho mọi thứ ổn định", nhưng các phương thức hoạt động của họ lại cho thấy một khía cạnh bí ẩn hơn.

Ngân hàng trung ương phối hợp chặt chẽ với chính phủ và giật dây chính sách tiền tệ, kiểm soát nguồn cung tiền thông qua các công cụ như lãi suất. Trong những thời điểm khủng hoảng, họ in tiền từ con số không và bơm vào nền kinh tế thông qua các ngân hàng thương mại, khiến mọi thứ có vẻ như vẫn ổn.

Họ không chỉ đơn thuần quan sát, ngân hàng trung ương còn điều tiết các ngân hàng thương mại, đặt ra luật chơi và can thiệp khi các ngân hàng gặp khó khăn (đóng vai trò là người cho vay cuối cùng). Mạng lưới kiểm soát này, tuy có vẻ như để bảo vệ hệ thống, nhưng lại khiến nền kinh tế và các ngân hàng ngày càng phụ thuộc vào họ hơn.

Hiểu được hàng nghìn tỷ đô la trong các gói kích thích đến từ đâu và ai là người quyết định cách phân bổ chúng là điều quan trọng để hiểu được hệ thống tài chính rộng lớn hơn. Chính phủ sử dụng một số công cụ để quản lý nguồn cung tiền tại những thời điểm cụ thể.

Ngân hàng trung ương và chính phủ có thể sử dụng các công cụ của chính sách tiền tệ và tài khóa để tác động đến nguồn cung tiền và nền kinh tế. Ví dụ, Cục Dự trữ Liên bang Hoa Kỳ (Fed) sử dụng chính sách tiền tệ để điều chỉnh lãi suất, ảnh hưởng đến cung tiền. Trong khi đó, chính sách tài khóa liên quan đến việc sử dụng các chính sách chi tiêu và thuế để tác động đến hoạt động kinh tế.

Tỷ lệ mục tiêu Chính sách tiền tệ

Tỷ lệ thất nghiệp dưới **6,5%**



2% - 3%
Tăng trưởng hàng năm của tổng sản phẩm quốc nội



Tỷ lệ lạm phát cơ bản trong khoảng **2,0% - 2,5%**

Mở rộng Chính sách tài khóa

Nhằm tăng chi tiêu tiêu dùng và đầu tư kinh doanh để thúc đẩy tổng cầu và tăng trưởng kinh tế.



VS

Thu hẹp Chính sách tài khóa

Nhằm giảm chi tiêu tiêu dùng và đầu tư kinh doanh để làm chậm lại tốc độ tăng trưởng kinh tế không bền vững và ngăn ngừa hoặc giảm thiểu lạm phát cao.



Tăng thuế

Tăng thuế

Tiền pháp định là gì và ai kiểm soát nó?

Chính sách tỷ giá hối đoái, cú sốc cung, và kiểm soát giá cả là những công cụ bổ sung để điều tiết nguồn cung tiền và tác động đến thương mại cũng như nền kinh tế. Mặc dù các chính sách này nhằm mục tiêu ổn định giá cả và kiểm soát lạm phát, nhưng sự can thiệp này thường dẫn đến các chu kỳ bùng nổ và suy thoái, gây ra nhiều thách thức cho tất cả những ai sử dụng đồng tiền bị kiểm soát.

Ví dụ: "Quá lớn để sụp đổ" (Too big to fail) đề cập đến những tổ chức tài chính có quy mô quá lớn và liên kết chặt chẽ đến mức việc sụp đổ của chúng sẽ gây ra hậu quả nghiêm trọng cho toàn bộ hệ thống tài chính. Trong cuộc khủng hoảng tài chính năm 2008, một số ngân hàng lớn được coi là "quá lớn để sụp đổ," khiến chính phủ Hoa Kỳ phải can thiệp và thực hiện các gói cứu trợ để ngăn chặn sự sụp đổ của họ.

Một trong những ví dụ nổi bật nhất về tổ chức "quá lớn để sụp đổ" trong cuộc khủng hoảng tài chính là ngân hàng đầu tư Lehman Brothers. Khi Lehman Brothers nộp đơn phá sản vào tháng 9 năm 2008, điều đó đã kích hoạt một hiệu ứng domino, bao gồm việc tập đoàn bảo hiểm khổng lồ AIG suýt sụp đổ và thị trường chứng khoán lao dốc mạnh. Chính phủ Hoa Kỳ đã buộc phải can thiệp và thực hiện các gói cứu trợ cho những tổ chức tài chính lớn khác nhằm ngăn chặn sự hỗn loạn tiếp theo và bảo vệ nền kinh tế rộng lớn hơn.

Hiểu cách các chính sách này hoạt động là điều cần thiết để nhận ra những hạn chế của hệ thống tiền tệ pháp định tập trung. Khi chưa hiểu rõ vấn đề, bạn sẽ khó nhận ra được giải pháp. Giờ đây, sau khi đã tìm hiểu cách hệ thống tiền pháp định vận hành trong quá khứ và hiện tại, chúng ta sẽ cùng khám phá viễn cảnh tương lai của tiền pháp định: Tiền kỹ thuật số của Ngân hàng Trung ương (CBDC).

4.3 Tiền kỹ thuật số của Ngân hàng Trung ương: Tương lai của tiền pháp định

Tiền kỹ thuật số của Ngân hàng Trung ương (CBDC) là bước tiến tiếp theo của các loại tiền pháp định. Thay vì kết hợp giữa tiền mặt (giấy, xu) và các hình thức thanh toán điện tử, CBDC là dạng tiền pháp định hoàn toàn kỹ thuật số, do chính phủ phát hành và được ngân hàng trung ương kiểm soát.

Hãy tưởng tượng loại tiền tệ bạn sử dụng hằng ngày nhưng không tồn tại dưới dạng vật lý — không còn xu trong túi hay tiền giấy để gấp lại. Điều khiến CBDC khác biệt chính là mức độ kiểm soát và giám sát cao hơn mà nó mang lại cho chính phủ và ngân hàng trung ương. Với CBDC, các cơ quan chức năng có được khả năng quan sát chưa từng có đối với các giao dịch tài chính, giúp việc theo dõi và điều tiết dòng tiền trở nên dễ dàng hơn.

Chính phủ và ngân hàng trung ương có thể dễ dàng điều chỉnh hình thức và nguồn cung của CBDC, thao túng lãi suất, và triển khai các công cụ chính sách tiền tệ và tài khóa với độ chính xác cao hơn. Về bản chất, CBDC cung cấp một phương tiện hiệu quả hơn để các cơ quan chức năng tác động và quản lý đồng tiền pháp định của mình.

Mặc dù CBDC được xem là tương lai của tiền pháp định, hệ thống tiền tệ hiện tại trên thế giới thực chất đã hoạt động hoàn toàn theo chuẩn tiền pháp định. Các loại tiền pháp định ngày nay không còn được gắn với vàng, dẫn đến việc nguồn cung tiền có thể được mở rộng đáng kể mà không chịu bất kỳ giới hạn thực sự nào.

Giờ đây khi bạn đã hiểu rõ hơn về cách hệ thống tiền pháp định vận hành, đã đến lúc khám phá những hệ quả của nó trong Chương 5.

Chương #5

Làm thế nào vẫn đề dẫn đến giải pháp

5.0 Giới thiệu về vấn đề

5.1 Sức mua giảm sút

5.1.1 Lạm phát tiền tệ và tác động đến sức mua

Hoạt động: Tác động của lạm phát — hoạt động đấu giá

5.2 Gánh nặng nợ toàn cầu và bất bình đẳng xã hội

5.2.1 Tác động đến cá nhân — mất sức mu

5.2.2 Tác động xã hội — bất bình đẳng giàu nghèo tăng

Hoạt động: Hậu quả của hệ thống tiền pháp định

5.2.3 Gánh nặng nợ toàn cầu

5.3 Những Cypherpunk và hành trình tìm kiếm tiền tệ phi tập trung

5.3.1 Những Cypherpunk

5.3.2 Hệ thống tập trung so với phi tập trung

5.3.3 Lược sử về tiền kỹ thuật số

Làm thế nào vấn đề dẫn đến giải pháp

5.0 Giới thiệu về vấn đề

Bất kỳ ai kiểm soát lượng tiền lưu thông trong một quốc gia đều nắm quyền kiểm soát tuyệt đối đối với toàn bộ ngành công nghiệp và thương mại... Khi bạn nhận ra rằng toàn bộ hệ thống này rất dễ bị chi phối, theo cách này hay cách khác, bởi một số ít người quyền lực ở tầng cao nhất, bạn sẽ không cần ai giải thích vì sao các thời kỳ lạm phát và suy thoái lại xảy ra.

James A. Garfield, Tổng thống Hoa Kỳ

Trong Chương 4, bạn đã biết rằng thế giới tài chính dựa vào một hệ thống có thể không vững chắc như người ta vẫn tưởng. Hệ thống tiền pháp định được duy trì bằng việc liên tục bơm thêm tiền giấy, dường như mang lại lợi ích cho một số ít người hơn là cho số đông. Chương này sẽ khám phá hệ thống tiền pháp định có ý nghĩa gì đối với người bình thường và toàn xã hội. Cuối cùng, chúng ta sẽ tìm hiểu câu chuyện về một nhóm người đã nhận ra những vấn đề này và âm thầm tìm kiếm một giải pháp có thể làm thay đổi tương lai của nhân loại.

5.1 Sức mua giảm sút

5.1.1 Lạm phát tiền tệ và tác động đến sức mua

Lạm phát tiền tệ là sự gia tăng lượng cung tiền trong một nền kinh tế, ảnh hưởng trực tiếp đến người dân bình thường bằng cách làm giảm sức mua của họ. Chu kỳ lạm phát giá bắt đầu khi có nhiều tiền hơn được đưa vào lưu thông. Điều này làm tăng nhu cầu đối với hàng hóa và dịch vụ, từ đó dẫn đến giá cả tăng lên.

Hãy tưởng tượng một nhóm bạn nhỏ — Alex, Bob và Charlie — mỗi người cầm một đô la trên tay, và chỉ có một chai nước được rao bán. Tình huống ban đầu rất đơn giản: ba người với tổng cộng ba đô la và một chai nước. Bây giờ, giả sử ai đó — hãy nói là chính quyền địa phương — quyết định tặng thêm cho mỗi người một đô la. Giờ đây, họ có tổng cộng sáu đô la. Với số tiền mới này, cả ba đều cảm thấy muốn mua chai nước duy nhất đó. Vì cả ba người đều muốn cùng một chai nước, họ bắt đầu trả giá cạnh tranh với nhau.

Nhu cầu tăng lên, được thúc đẩy bởi số tiền thêm vào, khiến họ đưa ra mức giá cao hơn so với giá ban đầu cho chai nước. Cuối cùng, cuộc đấu giá khiến giá chai nước tăng lên. Tình huống này phản ánh sự giảm sút sức mua của họ. Mặc dù có nhiều tiền hơn, họ không thể mua được nhiều chai nước như trước đây, thể hiện ảnh hưởng của lạm phát lên giá trị tiền của họ.

Trong ví dụ này, những người bạn đã trải nghiệm sự giảm sút sức mua vì họ đang sử dụng một hình thức tiền tệ bị ảnh hưởng bởi các yếu tố bên ngoài, chẳng hạn như số đô la thêm vào do chính phủ đưa ra. Việc không kiểm soát được cung tiền trên thị trường, kết hợp với nhu cầu tăng lên, đã dẫn đến giá cả tăng, khiến những người bạn khó mua được cùng một lượng hàng hóa với số đô la thêm vào.

Điều này minh họa cách sức mua của những người bạn bị ảnh hưởng bởi các yếu tố nằm ngoài tầm kiểm soát của họ, nhấn mạnh tầm quan trọng của việc hiểu và đặt câu hỏi về các hệ thống ảnh hưởng đến giá trị của đồng tiền chúng ta.

Bây giờ, hãy cùng khám phá cách điều này diễn ra trong đời thực.

Hoạt động: Tác động của lạm phát — hoạt động đấu giá

Mục tiêu: Hiểu được khái niệm lạm phát và cách nó ảnh hưởng đến giá cả hàng hóa và dịch vụ trong một nền kinh tế.

Định nghĩa:

 Nguồn cung tiền: Tổng lượng tiền đang lưu thông trong một nền kinh tế tại một thời điểm cụ thể.
Bao gồm:

- Tiền mặt vật lý, như tiền xu và tiền giấy
- Tài khoản thanh toán
- Tài khoản tiết kiệm
- Tài khoản thị trường tiền tệ
- Tiền gửi có kỳ hạn nhỏ (như chứng chỉ tiền gửi) dưới 100.000 đô la Mỹ

 Đấu giá: Một hình thức bán công khai, trong đó hàng hóa hoặc tài sản được bán cho người trả giá cao nhất.

Bài tập trên lớp — Làm theo hướng dẫn dưới đây:

1. Bạn sẽ nhận được một số tiền Cờ tỷ phú ngẫu nhiên từ giáo viên. Số tiền này đại diện cho nguồn cung tiền trong một xã hội.
2. Ghi lại tổng nguồn cung tiền vào bảng đã cung cấp.
3. Giáo viên sẽ tổ chức một phiên đấu giá thanh kẹo cho học sinh. Để giành được thanh kẹo, bạn sẽ cần đưa ra mức giá cao nhất bằng tiền Cờ tỷ phú của mình. Ghi lại mức giá thắng cuộc bên cạnh tổng nguồn cung tiền.
4. Sau đó, giáo viên sẽ thêm một lượng lớn tiền Cờ tỷ phú vào tổng nguồn cung. Điều này đại diện cho việc giá tăng nguồn cung tiền trong một nền kinh tế. Sau này, bạn sẽ tìm hiểu cách nguồn cung tiền được tăng hoặc giảm trong nền kinh tế.

Xã hội thường có thể khó lường và thiếu công bằng, được minh họa qua tình huống mô phỏng khi giáo viên ngẫu nhiên trao một lượng lớn tiền cho chỉ một số học sinh được chọn. Điều này phản ánh những tình huống thực tế, nơi sự phân bổ tài nguyên và cơ hội không đồng đều có thể xảy ra, làm nổi bật tính ngẫu nhiên và bất công vốn tồn tại trong nhiều hoàn cảnh.



5. Giáo viên sẽ tổ chức phiên đấu giá thứ hai cho một thanh kẹo khác, sử dụng cùng quy trình như trước. Ghi lại mức giá thắng cuộc bên cạnh tổng nguồn cung tiền trong bảng.
6. Giáo viên sẽ tiếp tục tổ chức phiên đấu giá lần thứ ba.

Làm thế nào vấn đề dẫn đến giải pháp

Vòng	Nguồn cung tiền	Mức giá thăng cuộc
1		
2		
3		

Kết luận:

- Việc giá tăng nguồn cung tiền đã ảnh hưởng như thế nào đến mức giá thăng cuộc cho các thanh kẹo?
- Mối quan hệ giữa nguồn cung tiền tăng và lạm phát là gì?
- Nguồn cung tiền có liên quan như thế nào đến đời sống thực?
- Khi một lượng tiền mới được bơm vào nền kinh tế, bạn nghĩ điều gì sẽ xảy ra với giá cả hàng hóa và dịch vụ? Bạn nghĩ sự thay đổi giá cả là tạm thời hay lâu dài, và tại sao? Theo bạn, sự thay đổi giá cả ảnh hưởng đến người dân như thế nào về lâu dài?

5.2 Gánh nặng nợ toàn cầu và bất bình đẳng xã hội

5.2.1 Tác động đến cá nhân — mất sức mua

Jaime là một sinh viên đại học sống trong một căn hộ nhỏ. Anh làm việc bán thời gian tại một quán cà phê để trang trải chi phí sinh hoạt và học phí. Ngay khi bắt đầu sống tự lập, Jaime đã trở nên giỏi quản lý số cái của mình.



Sổ cái là bản ghi chép chi tiết tất cả các giao dịch tiền tệ của bạn. Dù là tiền bạn kiếm được hay tiền bạn chi tiêu, sổ cái giúp bạn theo dõi tất cả.

Vào đầu năm 2023, anh ấy đã lên ngân sách 10.000 đô la cho chi phí sinh hoạt trong suốt cả năm, bao gồm tiền thuê nhà, thực phẩm và các nhu cầu thiết yếu khác. Đây là các giao dịch của anh trong tháng 1 năm 2023:

Ngày	Mô tả	Số tiền	Loại	Số dư
01/01/2023	Số dư ban đầu			1.600 USD
01/01/2023	Tiền thuê nhà tháng 1	800 USD	Ghi nợ	800 USD
05/01/2023	Đồ tạp hóa	100 USD	Ghi nợ	700 USD
15/01/2023	Lương bán thời gian	500 USD	Ghi có	1.200 USD
20/01/2023	Xăng xe	350 USD	Ghi nợ	850 USD
30/01/2023	Sách giáo khoa	150 USD	Ghi nợ	700 USD

Sổ cái này cho thấy số dư ban đầu của Jaime là 1.600 đô la, trong đó anh đã **chi** (ghi nợ) 800 đô la để trả tiền thuê nhà trong tháng. Sau đó, anh **chi** thêm 100 đô la cho đồ tạp hóa và nhận được **500 đô la** (ghi có) từ tiền lương làm bán thời gian, nâng số dư lên 1.200 đô la. Tiếp theo, anh **chi** tiền cho xăng xe và sách giáo khoa, làm số dư giảm xuống còn 700 đô la vào cuối tháng.

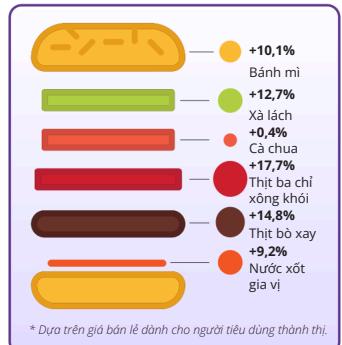
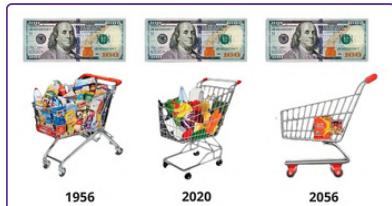
Mười hai tháng sau, Jaime đang ăn trưa với ông mình, người mà anh chia sẻ chi tiết về ngân sách cho năm 2024. Jaime nhận thấy ngân sách của mình không còn đủ như trước và chi phí sinh hoạt đã tăng đáng kể trong năm qua. Trong khi Jaime đang thắc mắc về điều này, ông của anh đã chỉ cho anh hình ảnh tiếp theo.

Jaime không thể tin vào mắt mình. Đây là lúc anh nhận ra rằng giá cả hàng hóa và dịch vụ tăng mạnh theo thời gian, dẫn đến việc sức mua của anh bị giảm đi.

Ông của Jaime nói: "Vào năm 1956, ông chỉ là một chàng trai trẻ mới bắt đầu vào đời. Ông nhớ khi đó mình kiếm được 380 đô la mỗi tháng khi làm công nhân trong nhà máy. Nghe thì có vẻ không nhiều, nhưng thời đó đó là một mức lương khá ổn. Thực tế là ông còn có thể tiết kiệm đủ tiền để mua một căn nhà riêng ở vùng ngoại ô."

Ông tiếp tục: "Chi phí mọi thứ trong thế kỷ trước rất khác so với bây giờ. Ví dụ, vào năm 2020, mua 30 thanh sôcôla Hershey's sẽ tốn 26,14 đô la. Tuy nhiên, nếu quay ngược thời gian về năm 1913, cùng số lượng thanh Hershey's đó chỉ có giá 1,00 đô la."

Sự chênh lệch đáng kể về giá này cho thấy sự thay đổi của sức mua theo thời gian và cách nó đã dịch chuyển qua các năm do lạm phát.

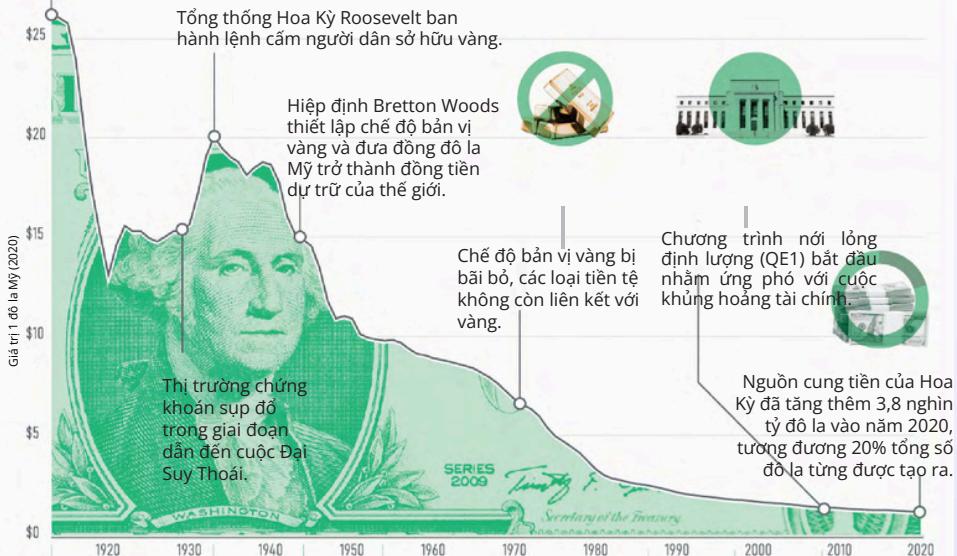


Làm thế nào vấn đề dẫn đến giải pháp

Giá trị của một đô la

Sức mua của đồng đô la Mỹ

Đạo luật Dự trữ Liên bang được ban hành, tạo ra một ngân hàng trung ương có khả năng quản lý nguồn cung tiền của quốc gia.



SỨC MUA CỦA 1 ĐÔ LA (TÍNH THEO ĐÔ LA 2020)



Jaime: "Giá cơ? Thật điên rồ. Cháu không thể tưởng tượng được tiền thuê nhà của mình lúc đó thấp hơn bấy giờ đến mức nào."

Ông: "Đúng vậy, tiền thuê nhà của cháu chắc chắn sẽ rẻ hơn nhiều lúc đó. Ông có một ví dụ khác để minh họa: hồi đó, 1 đô la có thể mua được khoảng 10 túi bánh quy pretzel. Năm 2020, ông phải trả 9,69 đô la cho cùng số lượng đó. Hãy tưởng tượng xem 10 túi bánh quy pretzel sẽ tốn bao nhiêu tiền ngày nay."

Chương #5



Jaime: "Wow, điều đó thật thú vị, ông ơi. Khi còn trẻ, ông đã trải qua điều này như thế nào vậy?"

Grandfather: "Ôi, Jaime, hồi ông còn trẻ thì mọi thứ rẻ hơn nhiều lắm. Một ổ bánh mì chỉ có 0,18 đô, còn một gallon xăng chỉ tốn 0,29 đô thôi. Thật không thể tin được chi phí sinh hoạt đã tăng cao đến mức nào."

Sau cuộc trò chuyện với ông mình, Jaime trở về nhà và xem lại sổ cái. Cậu nhanh chóng nhận ra rằng mình cần lập ngân sách thêm 1.000 đô la cho năm 2024 để có thể mua cùng một giỏ hàng hóa và dịch vụ như năm trước. Điều này có nghĩa là sức mua của cậu đã giảm đi 1.000 đô la vì giờ đây phải chi nhiều tiền hơn để mua cùng một lượng hàng hóa và dịch vụ. Trong khi mức lương của Jaime chỉ tăng nhẹ, thì chi phí sinh hoạt của cậu lại tăng vọt qua từng năm.

Bảng sau đây cho thấy chi phí sinh hoạt của Jaime trong năm đầu tiên và năm thứ hai, cùng với phần trăm giá tăng giá cả.

Để duy trì mức sống như cũ, Jaime sẽ phải làm việc nhiều giờ hơn mỗi tuần để kiếm thêm 1.000 đô la.

Dựa trên thông tin từ Cục Thống kê Lao động Hoa Kỳ, giá cả hiện nay cao gấp khoảng 30 lần so với năm 1913. Điều này có nghĩa là một đô la hiện tại chỉ có thể mua được khoảng 3% giá trị hàng hóa và dịch vụ so với thời điểm đó.

Hạng mục	Chi phí Năm thứ 1	Chi phí Năm thứ 2	% Tăng
Tiền thuê nhà	4.000 USD	4.500 USD	12,5%
Đồ tạp hóa	2.000 USD	2.300 USD	15%
Nhu yếu phẩm	4.000 USD	4.200 USD	5%
Tổng cộng	10.000 USD	11.000 USD	10%

Để minh họa, nếu ai đó cho Jaime lựa chọn du hành thời gian — hoặc nhận 100 đô vào năm 1913, hoặc đợi đến năm 2023 chỉ để nhận 3 đô la — thì điều này giống như phải chọn giữa một lần mua sắm thỏa thích trong quá khứ hay chỉ mua được vài món nhỏ ngày nay. Sự chênh lệch lớn về giá trị cho thấy sức mua của đồng tiền đã giảm đi nhiều theo thời gian.

CHI PHÍ SINH HOẠT NĂM 1938

SINH HOẠT

Nhà mới	\$3,900.00
Thu nhập trung bình	\$1,731.00 mỗi năm
Xe mới	\$860.00
Tiền thuê nhà trung bình	\$27.00 mỗi tháng
Học phí Đại học Harvard	\$420.00 mỗi năm
Vé xem phim	25¢ mỗi vé
Xăng	10¢ mỗi gallon
Tem thư Mỹ	3¢ mỗi con

THỰC PHẨM

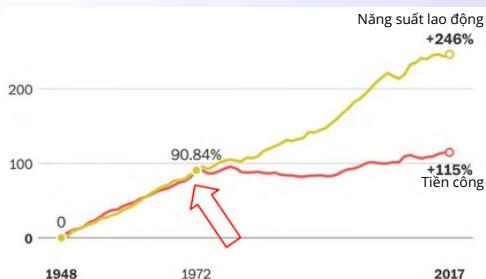
Đường cát trắng	59¢ cho 10 bảng
Sữa vitamin D	50¢ mỗi gallon
Cà phê xay	39¢ mỗi pound
Thịt xông khói	32¢ mỗi pound
Trứng	18¢ mỗi tá

(Dựa trên hình ảnh gốc)

Làm thế nào vẫn đền đến giải pháp

Nếu chỉ nhìn vào con số, Jaime kiếm được nhiều đô la hơn trong một năm so với ông của mình. Nhưng những đồng đô mà ông của Jaime sở hữu lại có giá trị cao hơn rất nhiều và có thể mua được nhiều thứ hơn vào thời đó.

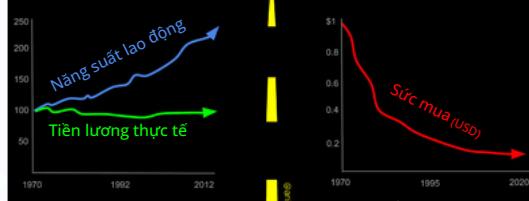
Tăng trưởng năng suất và tiền công theo giờ 1948 — 2017



LƯU Ý: Tiền công bao gồm lương và các phúc lợi cho lao động sản xuất và không giữ chức vụ quản lý.

Ví dụ của Jaime chỉ là một trong số rất nhiều. Trong thế giới tiền pháp định, việc các chính phủ tạo ra tiền từ hư không để phục vụ cho chương trình nghị sự của riêng họ là điều khá phổ biến, khiến người dân trên khắp thế giới phải gánh chịu hậu quả. Giá cả của các mặt hàng hàng ngày, từ bánh mì đến nhà ở, và từ hàng tạp hóa đến kỳ nghỉ đều tăng lên mỗi năm. Trong khi người giàu được hưởng lợi từ lạm phát nhờ sở hữu tài sản, thì người bình thường lại chứng kiến đồng tiền khó kiếm của mình dần mất giá. Kết quả là gì? Người dân và các gia đình trên toàn thế giới đang vật lộn vì sức mua suy giảm.

Con Đường Đến Chế Độ Nông Nô



Trong thế giới ngày nay, tác động đáng kể của lạm phát khiến nhiều người không còn muốn tiết kiệm tiền.

Thay vào đó, hầu hết đều chọn tiêu tiền ngay lập tức vì giá trị của nó giảm nhanh chóng. Cái nhìn bi quan này cần trở thành lập kế hoạch cho tương lai của họ.

Như thể hiện trong biểu đồ, mức lương trung bình của một người giàn như không tăng khi điều chỉnh theo lạm phát, nghĩa là họ không được tăng lương tương xứng với tốc độ mất giá của đồng tiền, dù họ làm việc chăm chỉ hơn.

Mọi người trên khắp thế giới đang phải làm nhiều việc hơn và làm việc nhiều giờ hơn chỉ để duy trì mức sống như cũ. Giống như đang chạy trên một chiếc máy chạy bộ — càng chạy nhanh hơn nhưng vẫn không thể tiến xa hơn. Hệ thống tiền pháp định khiến nhiều người cảm thấy như đang mắc kẹt trong một cuộc đua không hồi kết với giá cả ngày càng leo thang.

Trong nỗ lực theo kịp với chi phí ngày càng tăng, nhiều người phải dựa vào tín dụng, giống như dùng một miếng băng cá nhân nhỏ để che một vết thương rất sâu. Họ vay mượn hoặc đưa ra những quyết định bốc đồng chỉ để xoay xở qua ngày. Tiền nhanh trở thành một nhu cầu thiết yếu, và con người rơi vào vòng luẩn quẩn khi việc sinh tồn trước mắt quan trọng hơn việc lên kế hoạch cho tương lai.

Hệ thống tiền pháp định, với việc in tiền liên tục, ảnh hưởng đến tâm lý con người. Nó tạo ra thói quen ưu tiên thời gian cao – nghĩa là tập trung vào lợi ích ngắn hạn thay vì lập kế hoạch dài hạn. Giống như một giải pháp tạm thời để giảm bớt khó khăn trước mắt, người sống trong thế giới tiền pháp định thường đặt lợi ích trước mắt lên hàng đầu. Đó là bản năng sinh tồn, dẫn đến một vòng luẩn quẩn của sự phụ thuộc, nơi con người tìm mọi cách để có được tiền nhanh, dù điều đó không bền vững hay hiệu quả về lâu dài.

Về bản chất, tác động của hệ thống tiền pháp định vẽ nên một bức tranh đầy thách thức cho các cá nhân trên toàn cầu. Trong hệ thống tiền pháp định, giá cả tăng, thu nhập trì trệ và cuộc đấu tranh để sinh tồn trở thành cuộc chiến hàng ngày. Trong khi một số nhóm ngày càng giàu có hơn, hầu hết các cá nhân trên toàn thế giới vẫn phụ thuộc vào một hệ thống khiến họ ngày càng nghèo đi.

5.2.2 Tác động xã hội – bất bình đẳng giàu nghèo tăng

Trong một xã hội dựa trên tiền vững chắc, các quyết định tài chính của chính phủ phải gắn liền với sự đồng thuận của người dân. Tuy nhiên, trong hệ thống tiền pháp định, các chính phủ có thể vay nợ không giới hạn dựa trên gánh nặng của công dân.

Quyền in tiền tùy ý thường dẫn đến sự tập trung quyền lực chính trị. Hệ thống tiền pháp định cho phép các chính phủ tích lũy khoản nợ khổng lồ và đưa ra các quyết định mang lại lợi ích cho họ hơn là cho đa số người dân. Các siêu cường như Hoa Kỳ có được lợi thế cạnh tranh nhờ hiện tượng này. Họ có thể in tiền không giới hạn để tài trợ cho các kế hoạch của mình, bao gồm cả chiến tranh. Khả năng này giúp các quốc gia lớn kiểm soát, gây ảnh hưởng và tham gia vào các cuộc xung đột địa chính trị, tạo ra sự mất cân bằng quyền lực toàn cầu. Chiến tranh và các hành động nhằm kiểm soát người khác trở nên khả thi về mặt tài chính đối với các siêu cường, trong khi các quốc gia không có cùng mức độ linh hoạt tài chính lại bị hạn chế.

Dưới hệ thống tiền pháp định, của cải không được phân phối một cách đồng đều. Thay vào đó, nó có xu hướng tập trung vào tay một số ít người. Hiện tượng này giống như trò chơi Cờ tỷ phú, nơi chỉ một vài người chơi sở hữu gần như tất cả tài sản và tài sản, trong khi phần lớn còn lại phải vật lộn để tồn tại. Hệ thống tiền pháp định đã trở thành công cụ giúp một số nhóm nhất định tích lũy của cải. Việc in tiền cho phép các chính phủ và mối quan hệ chặt chẽ của họ với các ngân hàng trung ương bơm thêm tiền vào nền kinh tế, và những người nhận được khoản tiền mới tạo ra này chính là những cá nhân và tổ chức có sẵn tài sản và địa vị — những thực thể và cá nhân nắm giữ quyền lực. Họ hưởng lợi từ tiền mới trước khi các tác động tiêu cực như giảm sút mua bắt đầu lan rộng trong nền kinh tế.

Làm thế nào vấn đề dẫn đến giải pháp

Bất bình đẳng giàu nghèo không chỉ là câu chuyện giữa người có và người không có; mà còn là việc kìm hãm khả năng di chuyển kinh tế. Những người xuất thân từ hoàn cảnh ít thuận lợi ngày càng gặp nhiều khó khăn hơn trong việc leo lên bậc thang kinh tế, giống như bắt đầu một cuộc đua với chiếc ba lô nặng trên vai. Khoảng cách ngày càng lớn giữa giàu và nghèo gây ra nhiều vấn đề cho mọi người, khi những người giàu có định hình chính sách theo hướng có lợi cho họ. Điều này khiến cuộc sống của người dân bình thường trở nên khó khăn hơn, dẫn đến bất ổn xã hội, mất niềm tin vào các thể chế và các công đồng tan rã như tòa nhà bằng lá bài. Sự bất ổn của hệ thống tiền pháp định thể hiện qua sự không chắc chắn về kinh tế, bất ổn chính trị và những hậu quả toàn cầu khi thế giới phương Tây rơi vào suy thoái kinh tế.

Đây là một hiện tượng toàn cầu, ảnh hưởng đến cả các xã hội ở những quốc gia phát triển lẫn đang phát triển. Đôi khi, các cá nhân và nhóm giàu có lợi dụng cơ hội này để tận dụng hệ thống tài chính toàn cầu, điều này có thể làm khoảng cách giữa các tầng lớp giàu và nghèo càng thêm rộng.

Dưới hệ thống tiền pháp định, việc mắc nợ đã trở thành chuẩn mực của nhân loại. Các chính phủ, tổ chức, doanh nghiệp và cá nhân trên toàn thế giới thấy mình chìm trong biển nợ.

Sự thay đổi tâm lý hướng đến việc coi nợ là điều chấp nhận được bắt nguồn từ thiết kế của hệ thống tiền pháp định. Trong vài thập kỷ qua, các thực thể ngày càng dễ dàng vay nợ với quy mô lớn, và đối với người dân bình thường, việc này thường trở thành điều cần thiết do giá cả và chi phí sinh hoạt ngày càng tăng.

Chủ nghĩa tiêu dùng, tức là sự thõi thúc liên tục mua sắm và tiêu thụ, khiến con người mua nhiều hơn nhu cầu thực sự, dẫn đến tình trạng tiêu thụ quá mức và lãng phí. Dù có vẻ như một cuộc mua sắm không hồi kết, nhưng chi phí thực sự lại vượt xa giá tiền, ảnh hưởng đến sức khỏe tâm lý và tinh thần của con người.

Rõ ràng hệ thống tiền pháp định không chỉ là một cơ chế kinh tế đơn thuần. Thay vào đó, nó là một hệ thống định hình toàn bộ xã hội loài người. Từ sự tập trung quyền lực đến các động lực toàn cầu, bất bình đẳng giàu nghèo và các chuẩn mực xã hội, hệ thống tiền pháp định trực tiếp ảnh hưởng đến cách các quốc gia vận hành và cách người dân thường ngày định hướng cuộc sống của mình.

Hoạt động: Hậu quả của hệ thống tiền pháp định

- Có những hậu quả nào khác mà cá nhân và xã hội nói chung phải trải qua do hệ thống tiền pháp định gây ra?
- Hệ thống tiền pháp định đã để lại những hậu quả gì ở đất nước bạn? Trong suốt lịch sử, điều gì đã xảy ra và điều đó đã ảnh hưởng thế nào đến người dân trong nước bạn?
 - Ví dụ cá nhân: phiên tương tác



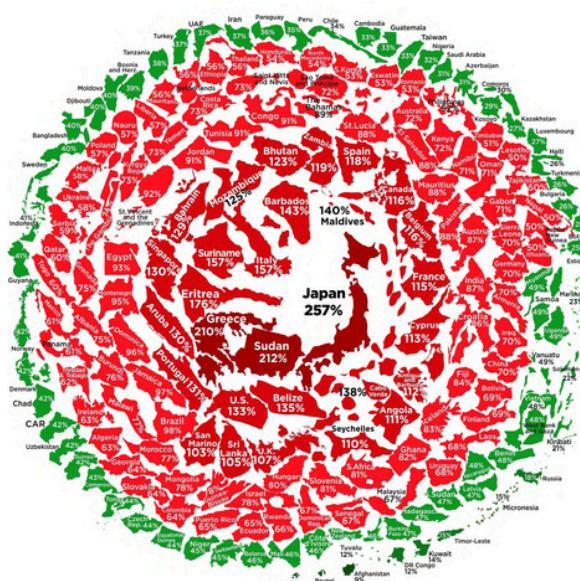
5.2.3 Gánh nặng nợ toàn cầu

Do hệ thống tiền pháp định, các chính phủ trên toàn cầu bị mắc kẹt trong một mạng lưới nợ khổng lồ, bị cuốn vào cái gọi là “vòng xoáy nợ toàn cầu.” Hãy tưởng tượng một tinh huống bạn vay nhiều tiền hơn khả năng trả nợ của mình. Điều này đang diễn ra trên quy mô rộng lớn trên toàn thế giới. Các chính phủ, chìm trong nợ nần, đang tham gia vào một trò chơi nguy hiểm khi tích lũy nhiều nợ hơn khả năng có thể trả. Đó là câu chuyện về chi tiêu bừa bãi, vay mượn và thiếu tăm nhinin, khiến các quốc gia trên thế giới đứng trước bờ vực thảm họa tài chính.



Tính đến nay, chính phủ liên bang Hoa Kỳ đã bổ sung thêm một khoản nợ khổng lồ lên tới 1 nghìn tỷ USD kể từ năm 2019. Tổng nợ đã tăng vọt từ khoảng 23 nghìn tỷ USD trong quý tư năm 2019 lên đến con số khổng lồ 34 nghìn tỷ USD hiện nay. Tốc độ các chính phủ trên toàn cầu tạo ra nợ mới không có dấu hiệu chậm lại; thực tế, nó đang tăng tốc. Năm 2023 được dự báo sẽ là năm tăng nợ nhiều nhất kể từ thời kỳ hỗn loạn của năm 2021, khi đại dịch COVID bùng phát.

Tình hình nợ Chính phủ trên thế giới



Vậy điều này có ý nghĩa gì đối với các cá nhân và xã hội vốn đã phải đổi mới với những hậu quả của hệ thống tiền pháp định? Vòng xoáy nợ mà họ bị cuốn vào giống như một quả bóng tuyết lăn xuống dốc — ngày càng lớn hơn và chúng ta không chắc làm thế nào để ngăn chặn nó.

Những hậu quả đã đề cập trước đó, từ bất bình đẳng giàu nghèo đến bất ổn xã hội, sẽ không biến mất. Thay vào đó, gánh nặng nợ toàn cầu đã đạt đến điểm không thể quay đầu, đảm bảo rằng mọi thứ sẽ ngày càng trở nên tồi tệ hơn.

Tỷ lệ nợ/GDP năm 2021 (%)



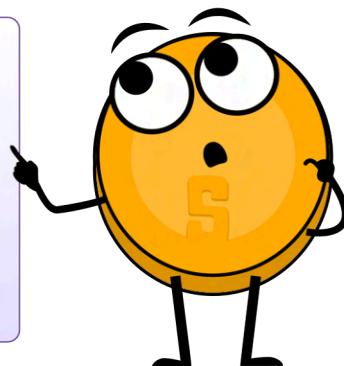
Làm thế nào vấn đề dẫn đến giải pháp



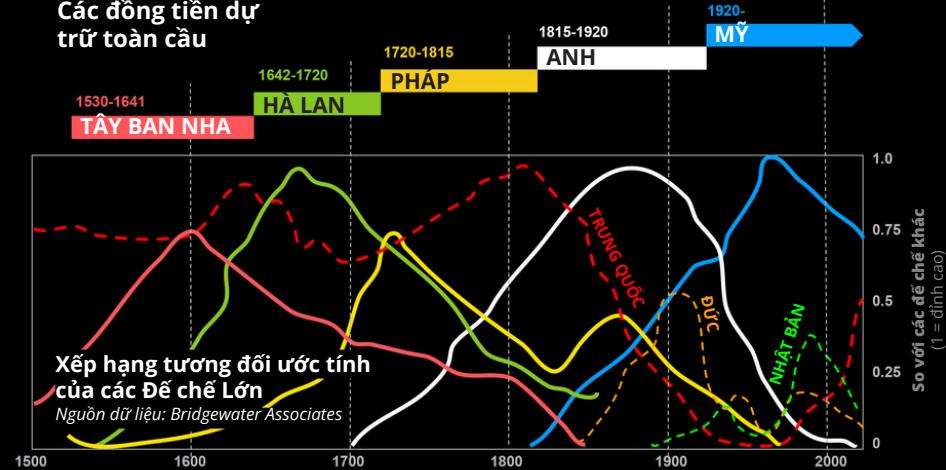
Tôi không tin rằng chúng ta sẽ bao giờ có đồng tiền tốt trở lại cho đến khi lấy quyền kiểm soát nó ra khỏi tay chính phủ... tất cả những gì chúng ta có thể làm là bằng một cách khéo léo, vòng vo, đưa vào một thứ mà họ không thể ngăn chặn được.

Friedrich Hayek

Người đoạt giải Nobel Kinh tế



Các đồng tiền dự trữ toàn cầu



5.3 Những Cypherpunk và hành trình tìm kiếm tiền tệ phi tập trung

Chúng ta đã chứng kiến quá trình tiền tệ dần bị các ngân hàng và chính phủ chi phối trong suốt chiều dài lịch sử, dẫn đến hệ thống tiền pháp định như hiện nay và những hậu quả nghiêm trọng mà nó mang lại cho xã hội. Nhưng sự phát triển của các công nghệ mới như mã hóa và internet đã cho phép những ý tưởng mới xuất hiện, như tiền kỹ thuật số độc lập — không bị chính phủ can thiệp, mở và ai cũng có thể tiếp cận. Giờ hãy cùng khám phá hành trình của những người đi đầu trong phong trào cách mạng này: những Cypherpunk.

5.3.1 Nhũng Cypherpunk



Máy tính có thể được sử dụng như một công cụ để giải phóng và bảo vệ con người, thay vì kiểm soát họ.

Hal Finney



Nửa sau thế kỷ 20 chứng kiến sự trỗi dậy của nhiều đột phá công nghệ như máy tính và internet, mở đường cho một kỷ nguyên số mới.

Một nhóm người đã nhận ra rằng những đổi mới to lớn này sẽ sớm biến đổi cách xã hội vận hành. Họ đã thấy trước cả tiềm năng và mối nguy hiểm của máy tính cá nhân, có thể là công cụ tạo điều kiện tự do để trao quyền cho cá nhân hoặc là công cụ kiểm soát và giám sát hoàn toàn.

Những người này được gọi là Cypherpunks. Họ xuất hiện như một nhóm lỏng lẻo gồm các nhà hoạt động, nhà mật mã học, lập trình viên và những người bảo vệ quyền riêng tư, cùng chung một tầm nhìn: theo đuổi quyền riêng tư, an ninh và một tương lai kỹ thuật số phi tập trung. Thuật ngữ "Cypherpunk" là sự kết hợp giữa "cypher" nghĩa là mã hóa mật mã và "punk" đại diện cho tinh thần phản văn hóa và nổi loạn.

Những người Cypherpunk tin tưởng vào sức mạnh của mật mã để bảo vệ tự do cá nhân. Mục tiêu của họ bao gồm phát triển các công cụ để bảo mật giao tiếp trực tuyến, ẩn danh hoạt động trên internet và thiết lập tiền kỹ thuật số hoạt động ngoài tầm kiểm soát của các cơ quan trung ương.

Những người Cypherpunk hiểu rõ hậu quả của hệ thống tiền pháp định và nhận thấy mối đe dọa từ một "tương lai Orwellian." Họ tin rằng họ phải đảm bảo rằng máy tính cá nhân và Internet sẽ trở thành những thứ tốt đẹp cho nhân loại thay vì là những công cụ có thể làm trầm trọng thêm sự kiểm soát của nhà nước đối với người dân.

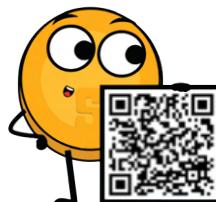


ĐỊNH NGHĨA VỀ “TƯƠNG LAI ORWELLIAN”:

“Tương lai Orwellian” chỉ một viễn cảnh phản ánh lối suy nghĩ và cảm hứng từ các tác phẩm của George Orwell. Thuật ngữ này liên quan đến một xã hội độc tài ác mộng, được đặc trưng bởi sự kiểm soát áp bức của chính quyền, giám sát rộng rãi, tuyên truyền và thao túng thông tin. “Orwellian” thường dùng để mô tả một kịch bản mà tự do và quyền tự chủ cá nhân của công dân bị hạn chế nghiêm trọng, tiếng nói phản kháng bị đàn áp, và thực tế bị bóp méo nhằm phục vụ lợi ích của một chế độ quyền lực và độc tài. Khái niệm này lấy tên từ George Orwell, người đã cảnh báo trong các tác phẩm của mình về những nguy cơ tiềm ẩn từ quyền lực nhà nước không được kiểm soát và sự xói mòn các quyền con người cơ bản.

Làm thế nào vấn đề dẫn đến giải pháp

Những nhân vật chủ chốt trong phong trào Cypherpunk bao gồm các tên tuổi nổi bật như Eric Hughes, Timothy C. May và John Gilmore. Năm 1992, Eric Hughes đã viết "Tuyên ngôn Cypherpunk," trong đó trình bày các nguyên tắc của nhóm. Tuyên ngôn nhấn mạnh tầm quan trọng của quyền riêng tư, mã hóa, và sự cần thiết để mỗi cá nhân tự kiểm soát danh tính kỹ thuật số của mình.



Hãy xem video này và khám phá câu chuyện về phong trào Cypherpunks!

Một trong những phát minh nổi bật nhất của phong trào Cypherpunks là việc tạo ra các công cụ và giao thức mật mã. Năm 1991, Phil Zimmermann đã giới thiệu PGP (Pretty Good Privacy – Bảo mật tương đối tốt), phần mềm mã hóa email trở thành dự án tiêu biểu. PGP cho phép người dùng gửi các tin nhắn được mã hóa qua internet mà chỉ người nhận dự kiến mới có thể giải mã. Trước đó, bất kỳ tin nhắn nào gửi qua internet đều có thể bị chặn và đọc bởi người khác, chẳng hạn như chính phủ.

Phong trào Cypherpunks cho rằng sự đột phá của mã hóa, cùng với internet và máy tính, đã tạo nền tảng vững chắc cho việc xây dựng các mạng lưới phi tập trung trong không gian kỹ thuật số, cho phép cá nhân giao tiếp và thực hiện giao dịch trên internet một cách riêng tư và không bị can thiệp bởi một cơ quan trung ương.

Những người theo chủ nghĩa Cypherpunk đã đi đúng hướng trong việc xây dựng một tương lai tươi sáng hơn cho nhân loại, nơi công nghệ sẽ là công cụ để tối đa hóa tự do thay vì kiểm soát. Những mảnh ghép còn thiếu chỉ là một mạng lưới phi tập trung và một loại tiền kỹ thuật số.

5.3.2 Hệ thống tập trung và phi tập trung

Hệ Thống Tập Trung: Một Kẻ Cầm Quyền, Muôn Vàn Vấn Đề

Trong một hệ thống tập trung, mọi thứ xoay quanh một cơ quan quyền lực chính, giống như một tòa nhà cao tầng ở giữa thành phố. Cơ quan này kiểm soát cách mà toàn bộ hệ thống vận hành. Hãy nghĩ đến các ngân hàng truyền thống như một ví dụ, nơi một nhóm nhỏ đưa ra tất cả các quyết định.



Ví dụ thực tế: Năm 2022, trong các cuộc biểu tình ôn hòa ở Canada, các ngân hàng đã đóng băng tài khoản của người biểu tình, cho thấy cách mà một cơ quan trung ương có thể can thiệp và kiểm soát quyền tiếp cận tài chính.



Những vấn đề của hệ thống tập trung:

- 👉 Điểm lỗi trung tâm: Nếu có sự cố xảy ra với cơ quan trung ương, toàn bộ hệ thống có thể sụp đổ.
- 👉 Kiểm soát: Một nhóm nhỏ ở cấp cao nắm toàn bộ quyền lực và thường đưa ra các quyết định có lợi cho họ hơn là cho số đông.
- 👉 Thiếu hiệu quả và có nhiều trung gian: Giống như kẹt xe trong thành phố, hệ thống tập trung có thể trở nên chậm chạp và tốn kém do có quá nhiều bên trung gian không cần thiết.
- 👉 Thiếu quyền tự chủ: Mọi người có thể không được tự đưa ra lựa chọn tài chính của mình; mọi thứ đều do cấp có thẩm quyền cao nhất quyết định.
- 👉 Kiểm duyệt và hạn chế: Cũng như một số khu vực trong thành phố có thể bị chặn, hệ thống tập trung có thể chặn hoặc giới hạn quyền truy cập vào một số nguồn tài chính.
- 👉 Thách thức về khả năng mở rộng: Khi có nhiều người cần sử dụng dịch vụ tài chính, hệ thống tập trung có thể không theo kịp nhu cầu.
- 👉 Rủi ro về bảo mật: Các vấn đề với cơ quan trung ương có thể khiến toàn bộ hệ thống dễ bị tấn công mạng.
- 👉 Thiếu minh bạch và lòng tin: Cách hoạt động bên trong của hệ thống tập trung thường khó hiểu, khiến người dùng khó đặt niềm tin vào nó.

Hệ thống phi tập trung: Quyền lực thuộc về người dân

Bây giờ, hãy tưởng tượng một hệ thống phi tập trung giống như một khu rừng lớn. Mỗi cái cây đại diện cho một phần riêng biệt, và toàn bộ khu rừng tượng trưng cho toàn hệ thống. Không giống như một thành phố chỉ có một điểm trung tâm, hệ thống phi tập trung giống như khu rừng bền bỉ, vẫn tồn tại được ngay cả khi một phần gặp sự cố.

- 👉 Ví dụ thực tế: Mạng Tor và trình duyệt của nó tạo ra một hệ thống phi tập trung, nơi mọi người có thể giữ ẩn danh trên internet và mạng này rất khó bị ngăn chặn hoặc kiểm duyệt.



Lợi ích của các hệ thống phi tập trung:

- 👉 Tăng khả năng chống chịu và độ tin cậy: Không có điểm lỗi trung tâm, nên hệ thống vẫn vững mạnh ngay cả khi gặp sự cố.
- 👉 Tăng cường bảo mật: Với các biện pháp mã hóa và bảo vệ phù hợp, hệ thống phi tập trung có khả năng chống lại sự kiểm soát từ một cơ quan duy nhất tốt hơn.

Làm thế nào vấn đề dẫn đến giải pháp

- Chủ quyền lớn hơn: Mọi người có nhiều quyền kiểm soát hơn đối với tiền bạc, dữ liệu và quyết định của mình.
- Tính minh bạch được cải thiện: Tất cả mọi người đều thấy cùng một thông tin, giúp hệ thống trở nên đáng tin cậy hơn.
- Tính không cần cấp phép và không giới hạn: Bất kỳ ai cũng có thể tham gia, tạo nên một hệ thống tài chính bao trùm.
- Cơ hội bình đẳng: Mọi người đều có cơ hội công bằng để đóng góp và lên tiếng.
- Tăng cường quyền riêng tư: Dữ liệu được phân tán cho nhiều người tham gia và phần lớn là ẩn danh, giúp hệ thống phi tập trung bảo mật hơn.

Dù hệ thống phi tập trung có nhiều lợi ích, việc ra quyết định chung có thể hơi phức tạp. Nó đòi hỏi mọi người phải cùng hợp tác.

Thay đổi Cách Quyền Lực Được Năm Giữ

Trong thế giới của các hệ thống tập trung và phi tập trung, vấn đề then chốt là quyền lực thuộc về ai. Các hệ thống tập trung trao quyền lực cho một nhóm nhỏ, trong khi các hệ thống phi tập trung phân tán quyền lực, để mọi người đều có tiếng nói. Sự chuyển dịch quyền lực này sẽ mở ra một tương lai công bằng và dân chủ hơn, nơi nhiều người có thể ảnh hưởng đến hệ thống định hình cuộc sống của họ.

5.3.3 Lược sử về tiền kỹ thuật số

Một trong những khái niệm then chốt mà những người theo chủ nghĩa Cypherpunk bàn luận là tiền kỹ thuật số. Họ nhận ra rằng nhà nước và tiền tệ cần phải tách biệt để đảm bảo tương lai mang lại lợi ích chung. Công trình đột phá của David Chaum về các giao thức mã hóa cho các giao dịch an toàn và riêng tư đã đặt nền móng cho điều này. Tuy nhiên, điểm hạn chế là giao thức này cần một cơ quan trung ương để vận hành hiệu quả, gây lo ngại về điểm yếu trung tâm và khả năng kiểm duyệt.

Trong những năm tiếp theo, nhiều người theo chủ nghĩa Cypherpunk đã cố gắng phát triển ý tưởng của nhau nhằm tạo ra một giải pháp khả thi cho tiền kỹ thuật số không bị kiểm soát bởi chính phủ. Bảng dưới đây mô tả một số đổi mới then chốt mà các Cypherpunk đã phát triển trong hành trình tìm kiếm tiền kỹ thuật số:

Tên và ngày	Mô tả	Hạn chế
E-Cash (1982)	E-Cash của David Chaum là một khái niệm sớm về tiền điện tử, tập trung vào bảo mật thông qua các kỹ thuật mã hóa.	Cần có cơ quan trung ương, gây lo ngại về điểm thất bại duy nhất và khả năng kiểm duyệt.
DigiCash (1990)	DigiCash, do David Chaum thành lập, nhằm tạo ra một dạng tiền kỹ thuật số với trọng tâm là quyền riêng tư.	Mô hình tập trung dẫn đến việc phá sản vào năm 1998.

B-money (1996)	B-money, do Wei Dai đề xuất, là một đề xuất lý thuyết về hệ thống tiền điện tử phân tán và ẩn danh.	Thiếu khả năng triển khai thực tế; vẫn là một ý tưởng khái niệm.
Hashcash (1998)	Hashcash, được phát triển bởi Adam Back, là hệ thống bằng chứng công việc (proof-of-work) nhằm hạn chế thư rác và các cuộc tấn công từ chối dịch vụ (DoS).	Không giải quyết trực tiếp vấn đề chi tiêu kép trong các loại tiền kỹ thuật số.
Bit Gold (1998)	Bit Gold, do Nick Szabo đề xuất, mô tả một hệ thống tiền kỹ thuật số phi tập trung với các yếu tố bằng chứng công việc.	Không bao giờ được triển khai thực tế, chỉ dừng lại ở mức ý tưởng lý thuyết.
e-Gold (2004)	e-Gold là một loại tiền kỹ thuật số tập trung được bảo chứng bằng vàng vật chất, cho phép người dùng mua và chuyển đơn vị e-Gold.	Các vấn đề pháp lý dẫn đến việc đóng cửa vào năm 2009, cho thấy những thách thức liên quan đến tiền tệ kỹ thuật số tập trung.

Bất chấp nhiều nỗ lực của những người theo chủ nghĩa Cypherpunk trong suốt nhiều thập kỷ nhằm tạo ra một loại tiền kỹ thuật số không chịu sự kiểm soát của bất kỳ nhóm hay chính phủ nào, những nỗ lực đó đã vấp phải nhiều thách thức thực tiễn và không thể hoàn toàn trở thành hiện thực. Những người Cypherpunk đã đến kết luận rằng việc xây dựng một dạng tiền kỹ thuật số vừa an toàn, vừa có thể mở rộng và có tiềm năng được chấp nhận rộng rãi là điều không hề dễ dàng.

Tuy nhiên, câu chuyện rẽ sang một hướng mới khi một cá nhân, học hỏi từ những bài học của những người theo chủ nghĩa Cypherpunk, đã nâng tầm khái niệm tiền kỹ thuật số phi tập trung lên một tầm cao mới. Trong các chương tiếp theo, chúng ta sẽ khám phá cách đóng góp của người này, dựa trên 40 năm nghiên cứu trước đó, cuối cùng đã dẫn đến sự ra đời của một hệ thống hoạt động hiệu quả.

Chương #6

Giới thiệu về

Bitcoin

6.0 Satoshi Nakamoto và sự ra đời của Bitcoin

6.1 Bitcoin hoạt động như thế nào?

6.1.1 Cơ chế đồng thuận Nakamoto (Nakamoto Consensus)

6.1.2 Những người chơi trò chơi

Hoạt động: Xây dựng đồng thuận trong mạng ngang hàng

6.2 Bitcoin như tiền kỹ thuật số có giá trị thực

6.2.1 Giới thiệu

6.2.2 Đặc điểm của Bitcoin

Hoạt động: Thảo luận lớp — Bitcoin có phải là tiền vững chắc không?

6.2.3 Chấp nhận trách nhiệm cá nhân

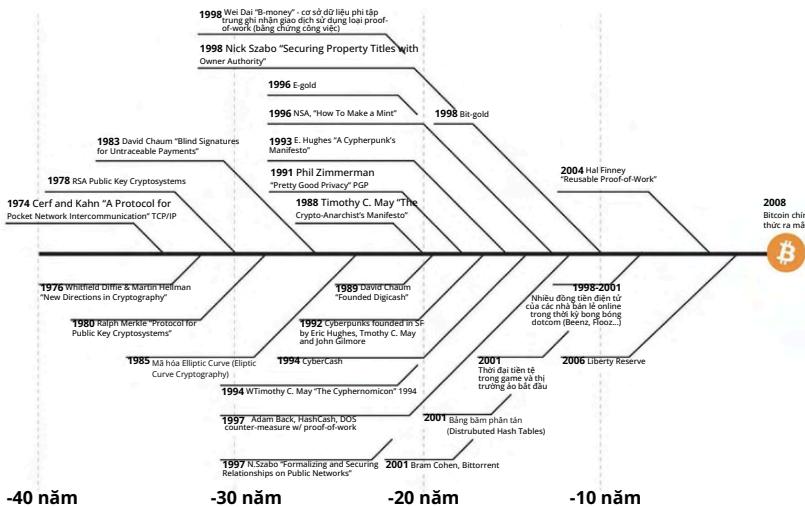
Giới thiệu về Bitcoin

6.0 Satoshi Nakamoto và sự ra đời của Bitcoin

Rất nhiều người tự động cho rằng tiền điện tử là một thất bại không thể cứu vãn do hàng loạt công ty đã phá sản kể từ những năm 1990. Tôi hy vọng điều rõ ràng là chính bản chất tập trung kiểm soát của những hệ thống đó đã khiến chúng thất bại. Tôi nghĩ đây là lần đầu tiên chúng ta thử một hệ thống phi tập trung không dựa trên niềm tin.

Satoshi Nakamoto

Tiền thân của Bitcoin: — Kết quả của 40 năm nghiên cứu, phát triển và nhu cầu

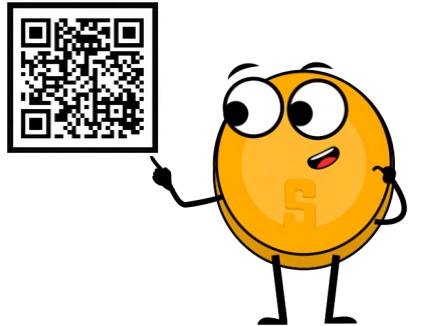


Như bạn đã đọc ở chương trước, nhiều Cypherpunk đã cố gắng tạo ra một hệ thống tiền tệ thay thế. Chương này tiếp tục câu chuyện của một trong số họ: một bộ óc đầy tầm nhìn có tên là " Satoshi Nakamoto." Nhân vật ẩn danh này (có thể là một người đàn ông, phụ nữ hoặc một nhóm người), từ lâu trước khi Bitcoin ra đời, đã là một người đam mê mật mã học, giống như các nhà khoa học máy tính và hacker, và đã tham gia vào các cuộc thảo luận nhằm tìm ra giải pháp thực tiễn để thay thế hệ thống tiền pháp định hiện tại.



Vào tháng 10 năm 2008, Nakamoto đã công bố một bản whitepaper mang tính đột phá có tiêu đề "Bitcoin: Hệ thống tiền điện tử ngang hàng" trên một danh sách thư điện tử chuyên về mật mã học. Tài liệu này đặt nền móng cho một giao thức ngang hàng phi tập trung, được thiết kế để hỗ trợ các giao dịch trực tuyến an toàn mà không cần bên trung gian.

Tâm nhìn của Nakamoto rất rõ ràng: tạo ra một phiên bản tiền điện tử hoàn toàn ngang hàng, không bị kiểm soát bởi các chính phủ quyền lực hay các tổ chức tài chính.



Chuyển nhanh đến ngày 3 tháng 1 năm 2009, khi Nakamoto đào khôi Bitcoin đầu tiên, được gọi là "khôi khởi nguyên" (genesis block). Đây là cột mốc đánh dấu sự ra mắt chính thức của mạng lưới Bitcoin, một hệ thống tiền tệ mới được xây dựng dựa trên niềm tin và tính bảo mật thông qua sổ cái phi tập trung. Trong những tháng và năm sau đó, ngày càng nhiều người đam mê đã tham gia và đóng góp vào ý tưởng này.

Bitcoin Genesis Block

Raw Hex Version

Năm 2011, sau khi mạng lưới Bitcoin chứng minh được khả năng vận hành thành công mà không cần sự hiện diện của người sáng lập quyền lực, Nakamoto đã gửi một email cho một nhà phát triển Bitcoin khác, thông báo rằng họ sẽ rút khỏi cộng đồng Bitcoin và trao tương lai của nó cho những “bàn tay tốt” khác cùng chung tầm nhìn.

Mặc dù đến tận ngày nay danh tính của Nakamoto vẫn còn là một bí ẩn, mục tiêu khi tạo ra Bitcoin của họ thì không hề mơ hồ. Về bản chất, Nakamoto tạo ra Bitcoin để lấy lại quyền lực từ một số ít và trao trả cho đa số, bằng cách tạo ra một hệ thống tiền tệ thay thế dưới dạng phi tập trung, mã nguồn mở và minh bạch, tách biệt tiền tệ khỏi nhà nước. Việc tạo ra Bitcoin là phản ứng của Nakamoto trước cuộc khủng hoảng tài chính năm 2008, cuộc khủng hoảng đã làm tổn thương người dân thường trên toàn thế giới trong khi làm giàu cho tầng lớp tinh hoa — một lần nữa. Bitcoin là câu trả lời của Nakamoto cho sự tham nhũng và tính dễ vỡ của hệ thống tiền pháp định. Nakamoto đã đặt nền móng cho một cuộc cách mạng mới và rồi rút lui thay vì nhận lấy công lao.

Giới thiệu về Bitcoin

Trong những năm tiếp theo, Bitcoin bắt đầu phát triển nhanh chóng và trở thành biểu tượng của hy vọng, sự trao quyền và tính kiên cường, thách thức hệ thống tiền pháp định và cung cấp một phương tiện giao dịch tài chính an toàn, chống kiểm duyệt. Bitcoin là một giao thức mã nguồn mở, có nghĩa là không ai có quyền sở hữu hay kiểm soát nó. Thiết kế của nó được công khai và mở để bất kỳ ai cũng có thể tham gia.

Ngày nay, giấc mơ của Nakamoto về một hệ thống tài chính không biên giới, minh bạch và an toàn vẫn tiếp tục sống động, thúc đẩy cuộc cách mạng tự do toàn cầu mà chúng ta đang chứng kiến. Mỗi ngày, người dân bình thường ngày càng lựa chọn rời khỏi hệ thống tiền pháp định và bước vào thế giới của Bitcoin. Các trung tâm Bitcoin — còn gọi là các nền kinh tế tuần hoàn Bitcoin — đã được những người yêu tự do khởi xướng ở nhiều vùng trên thế giới. Thậm chí cả những quốc gia tìm kiếm con đường thay thế, như El Salvador, cũng bắt đầu áp dụng Bitcoin theo cách riêng của họ.

6.1 Bitcoin hoạt động như thế nào?

6.1.1 Cơ chế đồng thuận Nakamoto (Nakamoto Consensus)

Bitcoin hoạt động như thế nào? Bitcoin có rất nhiều tính năng, và càng tìm hiểu càng thấy sâu rộng — rất sâu rộng. May mắn thay, nếu bạn mới bước vào thế giới Bitcoin lần đầu, bạn không cần phải hiểu hoàn toàn cách nó hoạt động để bắt đầu sử dụng.

Điều này cũng giống như khi sử dụng internet: hầu hết mọi người không biết chính xác giao thức TCP/IP hoạt động ra sao, nhưng họ vẫn gửi email, nhắn tin và đăng bài trên các mạng xã hội hàng ngày. Tương tự như vậy với việc lái xe — phần lớn mọi người không biết rõ chi tiết cách một chiếc xe hoạt động, nhưng họ biết cách lái xe.



Tuy nhiên, Bitcoin vẫn chưa được phổ biến rộng rãi. Nó vẫn là một công nghệ khá mới, giống như internet vào những năm 90. Vì lý do đó, việc hiểu những kiến thức cơ bản về Bitcoin một cách đơn giản, ít thuật ngữ kỹ thuật sẽ rất hữu ích.

Ý tưởng chính về cách Bitcoin hoạt động có thể tóm gọn trong một câu: Bitcoin là một sự đồng thuận giữa những người trực tuyến. Bạn có thể tưởng tượng nó giống như khi chơi một trò chơi bàn cờ cùng bạn bè. Với một trò chơi như Cờ tỷ phú, bạn và những người chơi khác đồng ý với các quy tắc cụ thể. Một trong những quy tắc của Cờ tỷ phú là chỉ chấp nhận các “tờ tiền Cờ tỷ phú” đặc biệt. Nếu James (một trong những người chơi) vi phạm quy tắc bằng cách dùng giấy vệ sinh để mua nhà thay vì dùng tiền Cờ tỷ phú, các người chơi khác sẽ gọi James là kẻ gian lận và sẽ ngừng chơi với anh ta. Tóm lại, để chơi trò chơi, bạn phải có sự đồng thuận về một bộ quy tắc chung và không được lệch khỏi những quy tắc đó, nếu không bạn sẽ bị loại bỏ.

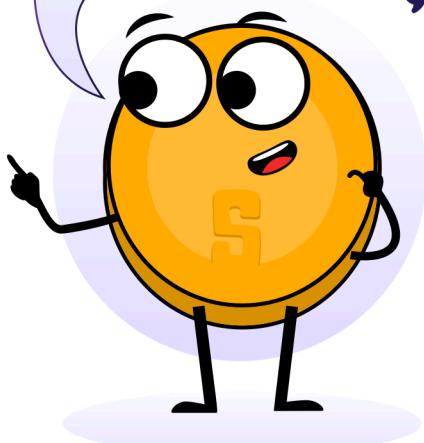
Về cơ bản, đó chính là cách Bitcoin hoạt động. Bitcoin là một mạng lưới những người cùng đồng thuận về một bộ quy tắc chung. Những quy tắc này được ràng buộc bằng toán học, được viết trong mã máy tính, và được tất cả những ai chạy phần mềm Bitcoin trực tiếp chấp nhận. Quy tắc của Bitcoin áp dụng bình đẳng cho tất cả người tham gia, có nghĩa là mọi người hoặc tuân theo quy tắc của trò chơi, hoặc sẽ không thể tham gia vì mạng lưới sẽ từ chối họ.

Ví dụ, một trong những quy tắc của Bitcoin là: “Sẽ không bao giờ có hơn 21 triệu đồng bitcoin.” Nếu ai đó muốn tự tạo thêm một triệu đồng bitcoin cho riêng mình, việc đó sẽ chẳng có ích gì vì họ sẽ ngay lập tức bị mọi người khác phát hiện và từ chối. Chính điều này làm cho Bitcoin trở nên vững chắc đến vậy.

Không quan trọng bạn là ai hay đến từ đâu; nếu bạn tham gia vào thế giới Bitcoin, bạn phải tuân theo cùng một bộ quy tắc như mọi người khác.

Điều này cũng áp dụng cho tất cả những cá nhân và tổ chức có quyền lực và tầm ảnh hưởng lớn trong thế giới tiền pháp định. Trong thế giới Bitcoin, không có chỗ cho gian lận hay phá hoại — mọi người đều được đối xử bình đẳng, và không ai có thể thay đổi điều đó.

“Bạn có biết rằng kể từ năm 2009, Bitcoin đã chống chịu hàng chục nghìn nỗ lực hack, can thiệp hoặc thay đổi hệ thống? Bitcoin đã chứng minh rằng không ai có thể ngăn chặn, kiểm soát hoặc thao túng nó.”



Giới thiệu về Bitcoin

6.1.2 Những người chơi trò chơi

Để hiểu rõ hơn về tính phi tập trung của Bitcoin, chúng ta cần tìm hiểu sâu hơn về các vai trò khác nhau trong mạng lưới. Trong thế giới Bitcoin, nhiều thành phần tham gia đảm nhận những vai trò riêng biệt nhưng phối hợp nhịp nhàng, góp phần vào hoạt động trơn tru của toàn bộ hệ thống.

1. Thợ đào: Kiến trúc sư của sự an toàn

Thợ đào là trụ cột của Bitcoin. Họ là những cá nhân hoặc nhóm người hoạt động phía sau hậu trường để duy trì và bảo vệ mạng lưới thông qua một cơ chế gọi là Bằng chứng công việc (Proof-of-Work – PoW). Những người tham gia này sở hữu các máy tính chuyên dụng với khả năng tính toán mạnh mẽ. Họ cung cấp sức mạnh xử lý của mình cho mạng lưới Bitcoin, cạnh tranh với nhau trong một "cuộc xô số toàn cầu" nhằm giành quyền thêm các khối giao dịch mới vào sổ cái phi tập trung của Bitcoin (blockchain). Sự cam kết của họ giúp đảm bảo tính bất biến của sổ cái và bảo vệ hệ thống khỏi các cuộc tấn công độc hại.

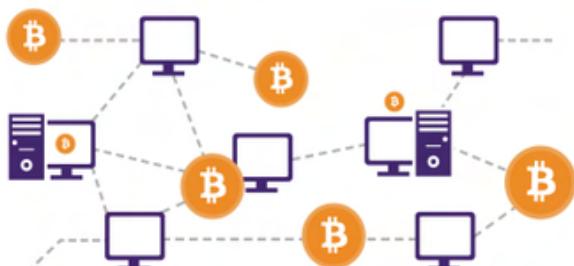


Bản chất phi tập trung của việc khai thác cho phép bất kỳ ai có đủ tài nguyên tính toán đều có thể tham gia. Nhờ sự nỗ lực của mình, những thợ đào giải được câu đố nhanh nhất sẽ được thưởng bằng bitcoin.

Các thợ đào Bitcoin phân bố khắp thế giới, bảo vệ mạng lưới khỏi sự tập trung và đảm bảo tính bảo mật của Bitcoin luôn mạnh mẽ và phân tán.

2. Nút mạng: Người gác cổng của việc xác thực

Các nút mạng Bitcoin là những người bình thường sống khắp nơi trên thế giới. Những người tham gia này đóng vai trò như "người gác cổng" của mạng Bitcoin bằng cách chạy phần mềm Bitcoin trên các máy tính cá nhân nhỏ của họ, nơi họ lưu giữ một bản sao toàn bộ sổ cái. Các nút xác thực giao dịch và đảm bảo tất cả người tham gia tuân thủ các quy tắc đồng thuận.



Bằng cách phân phối trách nhiệm xác thực trên toàn mạng lưới các nút, Bitcoin vẫn duy trì khả năng chống chịu các cuộc tấn công và giữ được bản chất không cần tin cậy. Các nút đóng vai trò quan trọng trong việc bảo vệ tính toàn vẹn của sổ cái, góp phần vào tinh thần phi tập trung của Bitcoin.

3. Người dùng: Những người tham gia được trao quyền

Người dùng — nguồn sống của mạng lưới Bitcoin — là những cá nhân tham gia các giao dịch. Bạn có thể xem người dùng như những người bình thường sống cuộc sống của họ, nhưng đồng thời đã tự trao quyền cho mình bằng cách tích hợp Bitcoin. Ví dụ, một số người dùng tiết kiệm tiền bằng bitcoin, trong khi những người khác, như công dân El Salvador, sử dụng bitcoin làm tiền để mua hàng tạp hóa và nhận lương bằng bitcoin.

Bitcoin trao quyền cho người dùng bằng cách loại bỏ sự cần thiết của các bên trung gian như ngân hàng và chính phủ, cho phép các giao dịch trực tiếp ngang hàng với nhau. Điều này cũng có nghĩa là người dùng hoàn toàn kiểm soát được tiền của mình và các giao dịch.

4. Nhà phát triển và dự án: Kiến trúc sư của sự đổi mới

Hệ thống tiền tệ của tương lai sẽ không tự xây dựng một cách tự nhiên, cũng như không thể được áp dụng rộng rãi trên toàn cầu một cách đúng đắn về mặt đạo đức nếu không có nỗ lực. Đó chính là vai trò của các nhà phát triển Bitcoin và các dự án liên quan.

Các nhà phát triển sử dụng chuyên môn kỹ thuật của mình để cải tiến và đổi mới giao thức Bitcoin. Họ đóng góp mã nguồn, đề xuất các cải tiến và khắc phục các điểm yếu, đảm bảo mạng lưới phát triển để đối phó với mọi thách thức. Bản chất mã nguồn mở của Bitcoin tạo điều kiện cho sự hợp tác, cho phép các nhà phát triển trên toàn thế giới cùng đóng góp vào sự phát triển của nó.

Vẻ đẹp của sự phát triển phi tập trung này là ngăn chặn việc một thực thể duy nhất kiểm soát độc quyền giao thức. Quá trình này diễn ra thông qua sự đồng thuận. Các nhà phát triển đề xuất ý tưởng và thay đổi, và chỉ những ý tưởng hay nhất, phù hợp với tầm nhìn chung về một thế giới tốt đẹp hơn mới nhận được sự ủng hộ từ cộng đồng, thúc đẩy sự phát triển minh bạch và dân chủ của Bitcoin cho đến khi sẵn sàng phục vụ 8 tỷ người.

Các dự án Bitcoin bao gồm nhiều nhóm khác nhau, từ các tổ chức phi lợi nhuận và tập đoàn có sứ mệnh rõ ràng đến các nhóm và cá nhân tạo ra nội dung giá trị. Những người này cùng làm việc hướng đến một mục tiêu hoặc trọng tâm cụ thể trong sứ mệnh lớn hơn của Bitcoin, đó là tự do chung của mọi người.

Các dự án Bitcoin đóng vai trò then chốt trong việc định hình và thúc đẩy việc áp dụng Bitcoin, hướng tới một tương lai ưu tiên trao quyền và tự do cho nhân loại.

Bản giao hưởng

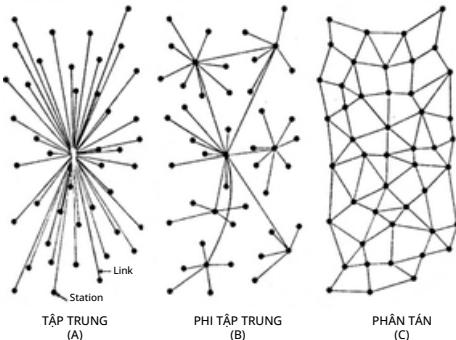
Tính phi tập trung của Bitcoin có thể được hình dung như một dàn nhạc giao hưởng mang tính hiệp lực, nơi mọi nhạc công khác nhau cùng tạo nên bản nhạc tuyệt đẹp nhất. Trong mạng lưới Bitcoin không có người lãnh đạo; thay vào đó, thư đào, các nút mạng, người dùng, nhà phát triển và các dự án đều đóng vai trò riêng của mình một cách đầy tính tự chủ và hợp tác.

Số cái phi tập trung được duy trì bởi các nút mạng đảm bảo tính minh bạch, trong khi cơ chế bằng chứng công việc (proof-of-work) mang lại sự bảo mật và ngăn chặn việc tập trung hóa hoạt động đào. Người dùng được trải nghiệm quyền tự chủ tài chính và được trao quyền, thoát khỏi sự kiểm soát của hệ thống tiền pháp định. Các nhà phát triển, được dẫn dắt bởi sự đồng thuận, đảm bảo giao thức luôn thích nghi để đáp ứng những nhu cầu đang thay đổi của nhân loại. Các dự án Bitcoin, theo cách riêng của mình, đóng góp vào sứ mệnh lớn hơn vì tự do tập thể.

Giới thiệu về Bitcoin

Như bạn có thể thấy, mỗi thành phần tham gia đều đóng vai trò quan trọng trong việc thúc đẩy sự chấp nhận Bitcoin và trao quyền cho con người. Mỗi người trong dàn nhạc phi tập trung này đều góp phần vào khả năng chống chịu và tuổi thọ lâu dài của Bitcoin, tạo nên một hệ sinh thái không cần lòng tin, không biên giới và đầy tính trao quyền.

Tóm lại, bản giao hưởng của sự phi tập trung trong Bitcoin vang lên như một minh chứng cho tầm nhìn của Satoshi Nakamoto và niềm đam mê mãnh liệt của cộng đồng toàn cầu đang hướng đến tự do và sự trao quyền.



Bài tập trên lớp — Xây dựng sự đồng thuận trong mạng ngang hàng



Mục tiêu

Hiểu cách một nhóm đạt được sự đồng thuận và tìm hiểu về mật mã học cũng như lớp đồng thuận trong Bitcoin.



Vật dụng

Thông điệp có chứa hướng dẫn được mã hóa và không mã hóa cho hành động ("tấn công" hoặc "không tấn công").



Chuẩn bị hoạt động

Giáo viên sẽ chọn một nhóm gồm ba hoặc bốn học sinh trước buổi học để đóng vai các nút độc hại trong hoạt động sau. Giáo viên sẽ giao một câu đố mật mã cho các node độc hại này như bài tập về nhà từ buổi học trước.

Các bước thực hiện:

- 1** Giáo viên sẽ chọn một học sinh trong nhóm làm "người khởi tạo" và trao cho học sinh này một mảnh giấy ghi thông điệp "TẤN CÔNG" cùng một chuỗi số, "4-16-14-21-1-21-21-1-3-11-".
- 2** Các học sinh sẽ đứng thành một vòng tròn trong khu vực được chỉ định. Những học sinh được chọn làm nút độc hại (malicious nodes) sẽ được sắp xếp cách xa nhau để tăng hiệu quả của bài học.



- 3** Khi cả nhóm đã đứng thành một vòng tròn, người khởi xướng sẽ chuyền mẫu giấy cho người đứng bên phải mình trong vòng tròn.
- 4** Sau khi mọi người đã đọc xong tin nhắn, người khởi xướng sẽ ra hiệu bằng cách nói "bây giờ," và cả nhóm sẽ đồng loạt phản ứng với nội dung tin nhắn. Nếu tin nhắn ghi "TẤN CÔNG," tất cả người tham gia sẽ bước lên một bước.
- 5** Sau phản ứng ban đầu, một số học sinh (những người nhận được tin nhắn mã hóa và giải mã đúng) sẽ đứng yên, trong khi những người còn lại làm theo hướng dẫn ban đầu, từ đó cho thấy sự thiếu đồng thuận.

Kết luận:

Thảo luận lý do tại sao không đạt được sự đồng thuận, giới thiệu khái niệm Vấn đề Các vị tướng Byzantine, cách nó liên quan đến nhu cầu về một mục tiêu chung, và sau đó phân tích cách Bitcoin đưa ra giải pháp cho vấn đề này.

Giới thiệu về Bitcoin

6.2 Bitcoin như tiền kỹ thuật số có giá trị thực

6.2.1 Giới thiệu

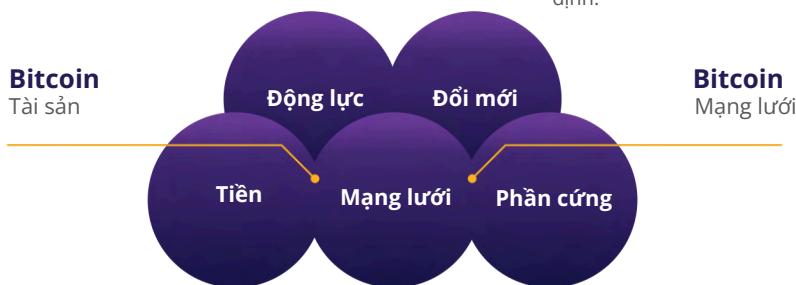
Hoạt động:

Xem video dài 1 phút 30 giây: "Bitcoin là gì?"



Nói một cách đơn giản, Bitcoin là tiền. Bitcoin không phải là một khoản đầu tư, mà là một cách tiết kiệm an toàn và trao quyền để bảo vệ số tiền bạn vất vả kiếm được.

Nắm giữ Bitcoin sẽ không làm bạn trở nên giàu có vì nó không tạo ra thêm Bitcoin cho bạn. Giá trị của nó, khi so sánh với tiền pháp định, có tăng lên, nhưng đó là do mức độ chấp nhận ngày càng tăng và sự mất giá của tiền pháp định.



Bitcoin là một hình thức tiền tệ mới; nó được gọi là "Internet của Tiền," có nghĩa là bất kỳ ai cũng có thể tham gia và bắt đầu trao đổi giá trị với những người dùng khác. Ngay cả những cộng đồng nghèo và bị cô lập nhất trên thế giới cuối cùng cũng có cơ hội tiếp cận một hệ thống tiền tệ. Cũng giống như bất kỳ ai có điện thoại và kết nối internet đều có thể sử dụng công cụ tìm kiếm, Bitcoin cho phép tất cả mọi người có điện thoại và internet tiếp cận một hệ thống tiền tệ toàn cầu mới.



Thanh toán nhanh hơn, rẻ hơn



Tài chính toàn diện



Tăng cường quyền riêng tư

Gửi tiền đi khắp thế giới chỉ trong vài phút, với chi phí cực thấp.

2,5 tỷ người không có tài khoản ngân hàng có thể tiếp cận tiền chí với một chiếc điện thoại hoặc máy tính.

Giao dịch Bitcoin là công khai nhưng danh tính của bạn thì không.

Bitcoin hoàn toàn là tiền kỹ thuật số và không biên giới. Bạn ở đâu không quan trọng vì Bitcoin tồn tại trên các máy tính và điện thoại thông minh khắp thế giới. Rất nhiều người dùng trên toàn cầu chạy phần mềm Bitcoin và lưu giữ một bản sao của sổ cái.

Phần mềm và bản ghi tất cả các giao dịch này gần như không thể mất đi vì có vô số bản sao được lưu trữ. Để ngừng hoạt động Bitcoin, bạn sẽ phải tắt toàn bộ Internet trên thế giới mãi mãi, điều này gần như không thể xảy ra.

Cuối cùng, Bitcoin là tài sản khan hiếm, nghĩa là số lượng token Bitcoin có thể tồn tại là hoàn toàn giới hạn. Không ai có thể làm giả Bitcoin — kể cả những chính phủ và tổ chức tài chính quyền lực nhất.

Nguyên tắc của Bitcoin



6.2.2 Đặc điểm của Bitcoin

Sự tiến hóa của tiền vững chắc

Như bạn đã học trong Chương 2, vòng đời của tiền vững chắc trải qua ba giai đoạn để được xã hội chấp nhận rộng rãi: từ việc là cất trữ giá trị, trở thành phương tiện trao đổi, và cuối cùng là đơn vị hạch toán toán.

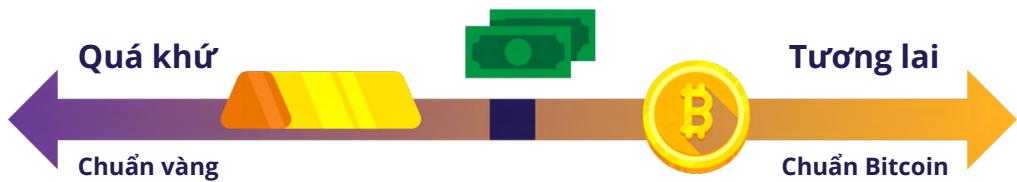
Giai đoạn đầu tiên của tiền tệ, cất trữ giá trị, là khi một loại tiền bắt đầu được tin tưởng như một tài sản ổn định (hoặc có giá trị tăng theo thời gian). Những người nhận ra điều này sớm sẽ tìm cách bảo vệ tài sản của mình bằng cách lưu trữ dưới dạng tiền này, đặc biệt trong những thời điểm bất ổn về địa chính trị và kinh tế vĩ mô.

Một số nhóm như các cơ quan truyền thông gọi Bitcoin là “vàng kỹ thuật số.” Điều này bởi vì Bitcoin đã khẳng định vững chắc vị thế là một cất trữ giá trị trong thập kỷ qua. Ngày càng có nhiều người xem Bitcoin như một công cụ phòng ngừa lạm phát, tương tự như vai trò của vàng trong lịch sử.

Giai đoạn tiếp theo là khi niềm tin vào sự ổn định của đồng tiền được củng cố. Đây là lúc đồng tiền chuyển mình thành phương tiện trao đổi, hỗ trợ các giao dịch trong đời sống hàng ngày. Trong giai đoạn này, tiền tệ bắt đầu được chấp nhận rộng rãi để trao đổi hàng hóa và dịch vụ.

Bitcoin đang dần tiến tới trở thành một phương tiện trao đổi. Với sự chấp nhận ngày càng tăng từ các thương nhân và sự phát triển của giao thức, các giao dịch Bitcoin ngày càng trở nên hiệu quả và phổ biến trong thương mại hàng ngày. Một ví dụ tiêu biểu là El Salvador, nơi Bitcoin được công nhận chính thức là tiền tệ hợp pháp. Mỗi ngày, ngày càng nhiều người dân và doanh nghiệp sử dụng Bitcoin như một phương tiện trao đổi.

Giới thiệu về Bitcoin



Ở giai đoạn cuối cùng, một loại tiền đạt được vị thế là đơn vị hạch toán toàn, trở thành thước đo chung để định giá hàng hóa và dịch vụ. Đây là giai đoạn mà nó trở thành tiêu chuẩn để so sánh và đo lường tất cả các giá trị khác.

Hành trình trở thành đơn vị hạch toán toàn là một quá trình dài hạn và kéo dài. Hiện tại, thế giới vẫn chỉ định giá hàng hóa và dịch vụ bằng các loại tiền pháp định, nên Bitcoin cần được chấp nhận rộng rãi hơn và tích hợp vào các hệ thống tài chính khác nhau. Tuy nhiên, nền tảng đã được xây dựng khi ngày càng nhiều doanh nghiệp và cá nhân bắt đầu xem xét và quy đổi giá trị theo Bitcoin.



Như bạn có thể thấy, Bitcoin đang trên đường tiến triển trong chu kỳ tiến hóa của tiền vĩnh chắc. Khi Bitcoin được tích hợp hoàn toàn vào hệ thống tài chính toàn cầu, nó có thể trở thành đơn vị hạch toán toàn tiêu chuẩn, từ đó tái định hình toàn bộ hệ thống tiền tệ toàn cầu.

Các tính chất của tiền

Như bạn đã học trong Chương 2, theo thời gian, con người đã nhận ra rằng tiền vững chắc phải sở hữu một số đặc điểm nhất định để hoạt động hiệu quả. Những đặc điểm đó bao gồm tính lâu bền, tính chia nhỏ, tính dễ mang theo, tính chấp nhận, tính khan hiếm và tính thay thế.

Hãy cùng xem Bitcoin có đáp ứng được các tiêu chuẩn này không.

Tính lâu bền: Bitcoin hoàn toàn là tiền kỹ thuật số nên có tính lâu bền tuyệt đối.

Tính chia nhỏ: Để so sánh, tiền pháp định USD có thể chia nhỏ đến cent (0,01). Bitcoin có thể chia nhỏ thành satoshi hay sat (0,00000001). Và nhờ tính chất kỹ thuật số, Bitcoin còn có thể chia nhỏ hơn nữa trong tương lai nếu con người cần. Hiện tại, Bitcoin là tài sản tiền tệ có khả năng chia nhỏ nhất trên thế giới.

Tính dễ mang theo: Vào tháng 4 năm 2020, có hơn 1,1 tỷ đô la được chuyển đi chỉ trong vài phút với chi phí chỉ 68 cent. Không có phương thức thanh toán nào khác có thể chuyển số tiền lớn như vậy với chi phí thấp và nhanh đến vậy, hoàn toàn tự động. Đây chính là lý do khiến Bitcoin trở thành hình thức tiền dễ di chuyển nhất trên thế giới.

Tính chấp nhận: Bitcoin vẫn đang trong giai đoạn đầu trở thành phương tiện trao đổi, và so với các loại tiền pháp định, tính chấp nhận hiện vẫn còn thấp.

Tính khan hiếm: Tổng số bitcoin tồn tại sẽ chỉ là 21 triệu đồng. Theo mã nguồn, không thể tăng số lượng này, có nghĩa là Bitcoin không chỉ khan hiếm mà còn là tài sản tiền tệ khan hiếm nhất thế giới.

Tính thay thế: Mỗi đơn vị bitcoin giống hệt các đơn vị khác và có thể trao đổi, giao dịch qua giao thức Bitcoin một cách tương đương, điều này làm cho Bitcoin trở thành một đồng tiền có tính thay thế cao.

Giới thiệu về Bitcoin

Bitcoin so với Vàng và Đô la Mỹ

Tính chất của tiền	Vàng	Tiền Pháp Định	Bitcoin
Tính lâu bền	Cao	Trung bình	Cao
Tính dễ mang theo	Trung bình	Cao	Cao
Tính chấp nhận	Trung bình	Trung bình	Cao
Tính thay thế	Cao	Cao	Cao
Tính khan hiếm	Trung bình	Thấp	Cao
Có thể xác minh	Trung bình	Trung bình	Cao
Lịch sử đã được kiểm chứng	Cao	Trung bình	Thấp
Chống kiểm duyệt	Trung bình	Trung bình	Cao
Thông minh / Có thể lập trình	Thấp	Trung bình	Cao

"Bitcoin vs Gold vs US Dollar" Bitcoin Magazine, <https://bitcoinnmagazine.com>

Bitcoin là một dạng tiền thông minh có thể lập trình, không thể bị tịch thu và có tất cả những đặc điểm giúp nó trở thành công cụ tiết kiệm tuyệt vời cũng như thuận tiện cho các thương nhân muốn giao dịch nhanh.

Vì là một số cái kỹ thuật số minh bạch, Bitcoin có thể rất hiệu quả trong việc phát hiện gian lận và đánh giá rủi ro trong các dịch vụ. Nó có những ưu điểm của vàng như số lượng giới hạn, nhưng cũng có lợi ích của tiền pháp định vì có thể chia nhỏ và dễ mang theo.Thêm vào đó, Bitcoin mang đến những tính năng mới phù hợp với thế giới kỹ thuật số ngày nay.

Bạn nghĩ sao? Bitcoin hiện chưa được công nhận và sử dụng rộng rãi, nhưng liệu nó có phải là tiền vững chắc?

Hoạt động: Thảo luận lớp — Bitcoin có phải là tiền vững chắc không?

Bây giờ khi chúng ta đã tìm hiểu kỹ hơn về Bitcoin, hãy cùng xem lại bảng so sánh tiền tệ từ Chương 2 và xem Bitcoin so với các hình thức tiền khác như thế nào:

Đặc điểm của tiền tốt	 Bò	 Thuốc lá	 Kim cương	 Euro	 Bitcoin
Bền					
Dễ mang theo					
Đồng nhất					
Được chấp nhận					
Khan hiếm					
Chia nhỏ					
Tổng					

6.2.3 Chấp nhận trách nhiệm cá nhân

Kết quả là một hệ thống phân tán không có điểm thất bại duy nhất. Người dùng giữ khóa mã hóa cho tiền của chính họ và giao dịch trực tiếp với nhau, nhờ mạng ngang hàng để kiểm tra việc chi tiêu kép.

Satoshi Nakamoto

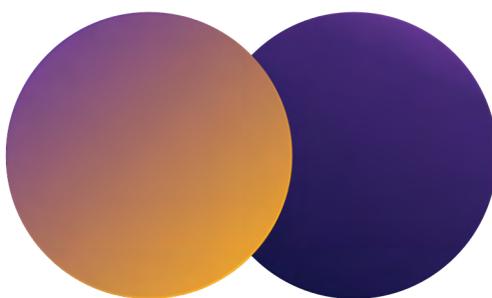
Giới thiệu về Bitcoin

Trong thế giới tiền pháp định, con người phụ thuộc vào chính phủ, ngân hàng và các nhà cung cấp dịch vụ thanh toán truyền thống. Những người đứng đầu các tổ chức tài chính này đặt ra các quy tắc của hệ thống và những người tham gia, phần lớn là công dân bình thường, buộc phải tuân theo. Dù bạn sống ở đâu, luôn có một bộ quy trình tiêu chuẩn hướng dẫn bạn phải làm gì và làm như thế nào. Theo thời gian, điều này đã dẫn đến một vòng luẩn quẩn đầy khó khăn, đặc biệt đối với các gia đình đang vật lộn với những thách thức ngày càng lớn trong cuộc sống hàng ngày.

Chính vì hệ thống này, con người đã quen với việc giao phó trách nhiệm tài chính của mình cho người khác. Ví dụ, hầu hết mọi người đều trông cậy vào người khác để được hỗ trợ, nhất là khi có sự cố xảy ra như mất quyền truy cập vào tài khoản ngân hàng.

**"Bitcoin sẽ bị
chặn lại"**

**Hiểu biết về
lịch sử tiền
tệ**



**"Bitcoin sẽ trở
nên lỗi thời"**

**Hiểu biết về
các mạng kỹ
thuật số**

"Bitcoin đã chiến thắng"

Như bạn đã biết, hệ thống tiền tệ của Bitcoin rất khác biệt. Bitcoin hoạt động theo một cách riêng, trong đó các nhà cai trị đã bị thay thế bởi một hệ thống quy tắc tự động. Không có người đứng đầu hay lãnh đạo nào, đồng nghĩa với việc không ai có thể áp đặt bạn phải làm gì. Nếu bạn muốn tận hưởng sự tự do và quyền làm chủ mới mẻ mà Bitcoin mang lại, bạn cần phải tìm hiểu cách nó hoạt động và áp dụng công nghệ này theo cách phù hợp với bản thân mình.



Đơn vị

xu Mỹ 0,01



Thanh toán



Phát hành



Sat
0,00000001



Với Bitcoin, bạn hoàn toàn kiểm soát được số tiền của mình, nhưng đi kèm với quyền kiểm soát này là trách nhiệm lớn hơn. Ví dụ, nếu bạn mất quyền truy cập vào bitcoins do mất khóa ví kỹ thuật số, nghĩa là bạn đã mất khoản tiết kiệm đó — vĩnh viễn. Không có tổng đài chăm sóc khách hàng để gọi hay ai đó để nhờ giúp — khi có vấn đề, bạn phải tự mình giải quyết.

May mắn thay, điều này sẽ không xảy ra với những ai quyết định chịu trách nhiệm hoàn toàn cho cuộc sống của mình. Việc sử dụng Bitcoin không hề phức tạp; nó chỉ là một khái niệm mới. Mọi khó chịu đều xuất phát từ sự chưa quen thuộc, nhưng nếu bạn sẵn sàng học cách sử dụng Bitcoin và chấp nhận trách nhiệm bảo vệ tài sản của mình, Bitcoin sẽ trở thành công cụ trao quyền — bạn làm chủ, không ai có thể chiếm đoạt tài sản của bạn.

Tóm lại, chìa khóa nằm ở hành động, hiểu biết cách Bitcoin vận hành và áp dụng nó theo nhu cầu cũng như triết lý sống riêng của bạn. Tiếp theo, chúng ta sẽ bắt đầu sử dụng bitcoin bằng cách tạo ví Bitcoin, gửi và nhận giao dịch đầu tiên, đồng thời xem xét các phương pháp bảo mật tốt nhất.

Chương #7

Cách sử dụng Bitcoin

7.0 Giới thiệu

7.1 Mua và trao đổi Bitcoin

7.1.1 Giao dịch ngang hàng (P2P): Trực tiếp

7.1.2 Giao dịch ngang hàng (P2P): Trực tuyến

7.1.3 Sàn giao dịch tập trung

7.2 Giới thiệu về ví Bitcoin

7.2.1 Ví tự lưu ký và ví lưu ký

7.2.2 Các loại ví Bitcoin khác nhau

7.2.3 Mã nguồn mở và mã nguồn đóng

Hoạt động: Đánh giá ví Bitcoin trong lớp học

7.3 Thiết lập ví bitcoin di động

Hoạt động: Thiết lập và khôi phục ví Bitcoin

7.4 Nhận và gửi giao dịch

Hoạt động: Giao dịch Bitcoin trong thực tế

7.5 Tiết kiệm bằng Bitcoin

7.6 Đừng tin, hãy xác minh

Cách sử dụng Bitcoin

7.0 Giới thiệu

Tại sao ai đó lại tin vào tiền của mày anh mợt sách thay vì tiền của ngân hàng trung ương? Một sách mang đến cho bạn internet. Còn ngân hàng mang đến cho bạn cuộc

Đại Khủng Hoảng.

Andreas M. Antonopoulos

Bây giờ, khi bạn đã hiểu rõ hơn về Bitcoin và mục đích của nó, đã đến lúc tìm hiểu cách sử dụng Bitcoin trong thực tế. Trong chương này, chúng tôi sẽ hướng dẫn bạn từng bước cách mua Bitcoin, khám phá các loại ví khác nhau, hỗ trợ bạn thiết lập ví Bitcoin riêng, và thậm chí thực hành gửi cũng như theo dõi một giao dịch Bitcoin trên mạng lưới. Đã đến lúc biến kiến thức của bạn thành hành động!

7.1 Mua và trao đổi Bitcoin

Có nhiều cách để bạn có thể mua Bitcoin. Ví dụ, bạn có thể:

- ◆ Nhận thanh toán bằng Bitcoin cho công việc của bạn và thanh toán cho sản phẩm hoặc dịch vụ của người khác bằng Bitcoin (xem thêm ở Chương 8)
- ◆ Đào Bitcoin (xem thêm ở Chương 9)
- ◆ Đổi tiền pháp định lấy Bitcoin hoặc đổi Bitcoin lấy tiền pháp định trực tiếp (giao dịch trực tiếp với người khác)
- ◆ Đổi tiền pháp định lấy Bitcoin hoặc đổi Bitcoin lấy tiền pháp định thông qua các nền tảng trực tuyến.



Dưới đây, chúng ta sẽ tìm hiểu cách đổi tiền pháp định lấy Bitcoin và ngược lại, thông qua cả giao dịch trực tiếp và các phương thức trực tuyến, vì đây là những lựa chọn phổ biến nhất.

7.1.1 Giao dịch ngang hàng: Trực tiếp

Tham gia vào các giao dịch ngang hàng (P2P) để mua và bán Bitcoin nghĩa là bạn trực tiếp trao đổi tiền pháp định (hoặc hàng hóa, dịch vụ khác) lấy Bitcoin với một cá nhân khác, mà không cần đến sự tham gia của ngân hàng hay bên trung gian nào.

Cả hai bên sẽ cùng thỏa thuận về số lượng và tỷ giá trao đổi. Người mua đưa tiền mặt, người bán chuyển Bitcoin, và giao dịch kết thúc. Mặc dù việc trao đổi ngang hàng thường dễ thực hiện hơn khi gặp trực tiếp ngoài đời thực, bạn cũng có thể thực hiện từ bất kỳ đâu nhờ vào internet. Ngoài ra, việc đổi Bitcoin lấy tiền pháp định cũng diễn ra theo quy trình tương tự nhưng ngược lại.



7.1.2 Giao dịch ngang hàng: Trực tuyến

Xuất hiện các nền tảng P2P, nơi người mua và người bán Bitcoin gặp nhau trên không gian mạng để thực hiện giao dịch trực tiếp trên internet mà không cần trung gian.

Với những nền tảng này, bạn không phải tin tưởng ai về thông tin hay tiền của mình; bạn có thể gặp gỡ các đối tác ngang hàng khác và giao dịch trực tiếp với họ.



Trên hầu hết các nền tảng P2P, các đối tác ngang hàng phải đặt cọc một phần tiền để đảm bảo họ sẽ thực hiện đúng cam kết của mình. Đặt cọc (escrow) nghĩa là gửi tiền vào một nơi an toàn do nền tảng kiểm soát cho đến khi cả hai bên hoàn thành nghĩa vụ. Nó giống như một người bạn đáng tin cậy giữ tài sản của bạn cho đến khi mọi người đều giữ lời hứa.

7.1.3 Sàn giao dịch tập trung

Sử dụng các sàn giao dịch tập trung có thể là cách dễ nhất để mua và bán Bitcoin, nhưng đồng thời cũng đi kèm với những đánh đổi đáng kể. Các sàn giao dịch tập trung là các công ty cho phép khách hàng mua bán Bitcoin trực tiếp thông qua họ. Tuy nhiên, sự tiện lợi này cũng có cái giá của nó.



TẬP TRUNG

Sàn Giao Dịch Tập Trung và Những Đánh Đổi

Cần lưu ý rằng khi mua Bitcoin qua sàn giao dịch tập trung, bạn thường phải cung cấp thông tin cá nhân và xác minh danh tính. Điều này tạo ra nguy cơ bị đánh cắp danh tính và làm lộ thông tin cá nhân trước các mối đe dọa tiềm ẩn.Thêm vào đó, các sàn giao dịch tập trung giữ Bitcoin của bạn, có nghĩa là bạn không kiểm soát tiền của mình cho đến khi rút khỏi sàn.

Thêm vào những lo ngại này, các sàn giao dịch tập trung có thể chiếm đoạt tiền của người dùng hoặc cho vay nhiều Bitcoin hơn số dự trữ mà họ có cho đến khi phá sản. Đúng vậy, giống như các ngân hàng! Tuy nhiên, trong thế giới Bitcoin, không có ngân hàng trung ương nào để cứu các ngân hàng gian lận bằng cách in thêm tiền, vì bạn không thể in thêm Bitcoin!

Cách sử dụng Bitcoin

7.2 Giới thiệu về ví Bitcoin

Không giống như tiền vật lý, Bitcoin thực sự không nằm trong ví Bitcoin. Thay vào đó, chúng tồn tại trên số cái phân tán mà mạng lưới Bitcoin liên tục xác minh và bảo mật. Vậy, làm sao bạn có thể sở hữu Bitcoin?

Bạn chỉ thực sự sở hữu Bitcoin khi bạn nắm giữ khóa riêng (private key) cho phép bạn ký giao dịch và chuyển quyền sở hữu Bitcoin cho người khác. Đây chính là hành động gửi Bitcoin.

Với điều đó trong tâm trí, hãy cùng tìm hiểu hai khái niệm mà chúng ta đề cập đến khi sử dụng thuật ngữ “ví”:



- ◆ Một khóa riêng chính (giống như mật khẩu) cho phép bạn tạo ra các khóa công khai mà bạn có thể chia sẻ với người khác để nhận và gửi Bitcoin.
- ◆ Giao diện trên thiết bị di động hoặc máy tính cho phép bạn tương tác với mạng lưới Bitcoin để kiểm tra số dư Bitcoin của mình, gửi và nhận giao dịch, cũng như phát giao dịch đó lên mạng. Các loại ví khác nhau, cùng với ưu điểm và hạn chế của chúng, sẽ được trình bày trong phần tiếp theo.

7.2.1 Ví tự lưu ký và ví lưu ký

Trước khi đi vào chi tiết các loại ví Bitcoin và đặc điểm của chúng, chúng ta cần phân biệt rõ giữa ví tự lưu ký và ví lưu ký, như được trình bày trong bảng dưới đây. Bạn có thể thấy được lợi ích và rủi ro của từng loại ví cũng như ai là người kiểm soát Bitcoin trong mỗi trường hợp. Ví tự lưu ký nghĩa là người dùng nắm giữ khóa riêng, đồng nghĩa với việc họ thực sự sở hữu Bitcoin của mình, trong khi với ví lưu ký, một bên thứ ba sẽ giữ Bitcoin thay cho người dùng.

Loại ví	Ai kiểm soát Bitcoin của tôi?	Lợi ích	Rủi ro
Ví tự lưu ký	Người dùng	Toàn quyền kiểm soát tiền và giao dịch, không cần qua quy trình phê duyệt hay bị đóng băng tài khoản, không bị kiểm soát bởi công ty hay chính phủ, được bảo vệ khỏi việc tịch thu tùy tiện, giống như giữ tiền mặt tại nhà.	Không thể khôi phục nếu mất cụm từ khôi phục, ít hỗ trợ khách hàng, toàn bộ trách nhiệm thuộc về người dùng.
Ví lưu ký	Bên cung cấp dịch vụ thứ ba	Dễ dàng khôi phục nếu mất quyền truy cập, hỗ trợ khách hàng thuận tiện hơn.	Tiền luôn được kết nối với internet nên dễ bị hack và xâm nhập trái phép. Bên lưu ký kiểm soát và có thể đóng băng tài khoản.

Trong ví tự lưu ký (còn gọi là ví không lưu ký), chỉ có bạn mới giữ các khóa của ví và bạn hoàn toàn kiểm soát mọi hoạt động ra vào ví. Ngược lại, trong ví lưu ký, một người khác giữ khóa riêng, cho phép họ toàn quyền truy cập và di chuyển bất kỳ Bitcoin nào mà ví đó kiểm soát thay cho bạn.

-  Tự lưu ký giống như việc bạn trở thành ngân hàng của chính mình. Giao dịch không chịu sự kiểm soát hay quyền hạn của bất kỳ chính phủ hay công ty nào, nhưng đồng thời bạn cũng phải hoàn toàn chịu trách nhiệm trong việc giữ an toàn cho Bitcoin của mình.
-  Tự lưu ký đảm bảo rằng bên thứ ba không thể tịch thu Bitcoin của bạn khi chưa có sự đồng ý của bạn.
-  Tự lưu ký mang lại sự yên tâm trong những thời điểm không chắc chắn, vì bạn biết rằng Bitcoin của mình được bảo vệ an toàn.

Việc chọn đúng loại ví phù hợp với nhu cầu của từng người là rất quan trọng. Đôi khi, mọi người gặp khó khăn trong việc phân biệt liệu họ đang cài đặt ví tự lưu ký hay ví lưu ký. Bảng dưới đây cho thấy sự khác biệt trong quá trình cài đặt.

Loại ví	Bước 1: Chọn ví	Bước 2: Cài đặt ví	Bước 3: Tạo ví mới	Bước 4: Bảo mật cụm từ seed	Bước 5: Bắt đầu sử dụng ví
Ví tự lưu ký	Chọn nhà cung cấp ví tự lưu ký	Làm theo hướng dẫn của nhà cung cấp ví	Tạo cụm từ khôi phục và ít nhất một khóa riêng	Lưu cụm từ khôi phục ở nơi an toàn	Bắt đầu sử dụng ví để nhận và gửi bitcoin
Ví lưu ký	Chọn nhà cung cấp ví lưu ký	Làm theo hướng dẫn của nhà cung cấp ví	Tạo tài khoản với nhà cung cấp ví	Không áp dụng (nhà cung cấp giữ khóa riêng)	Bắt đầu sử dụng ví để nhận và gửi bitcoin



KHÔNG GIỮ KHÓA KHÔNG GIỮ TIỀN

"Không giữ khóa, không giữ tiền" là một câu nói phổ biến trong cộng đồng người dùng Bitcoin. Nó thể hiện quan điểm rằng nếu bạn không trực tiếp kiểm soát khóa riêng của ví Bitcoin thì bạn cũng không thực sự sở hữu số Bitcoin đó.

Ai có quyền truy cập vào khóa riêng của bạn sẽ có quyền sở hữu Bitcoin của bạn. Vì vậy, việc bảo vệ khóa riêng khỏi những con mắt tò mò là điều vô cùng quan trọng. Chúng ta sẽ cùng tìm hiểu một vài cách để làm điều đó trong những phần sau của cuốn sách.

Từ phần này trở đi, chúng ta sẽ chỉ nói đến ví tự lưu ký, nơi người dùng sở hữu khóa riêng và hoàn toàn kiểm soát Bitcoin của mình.

Đừng lo lắng nếu mọi thứ có vẻ phức tạp hoặc bạn chưa hiểu hết. Đây là một hành trình, và bạn sẽ hiểu rõ hơn khi bắt đầu sử dụng Bitcoin nhiều hơn!

Cách sử dụng Bitcoin

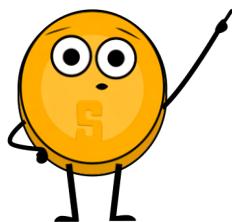
7.2.2 Các loại ví Bitcoin khác nhau

Tùy vào nơi khóa riêng của bạn được tạo ra và lưu trữ, chúng ta thường sử dụng những tên gọi khác nhau để mô tả các loại ví Bitcoin. Nếu khóa được lưu trên điện thoại thông minh, ta gọi đó là "ví di động." Nếu được lưu an toàn trên một thiết bị chuyên dụng, đó là "ví cứng." Còn nếu khóa chỉ được lưu trên giấy, thì gọi là "ví giấy."

Các tên gọi khác nhau của ví Bitcoin tùy theo cấu trúc của chúng:

Loại ví	Mô tả	Ưu điểm	Nhược điểm	Người dùng ví dụ
Ví trực tuyến	Một loại ví được truy cập thông qua trình duyệt web.	Có thể truy cập từ bất kỳ thiết bị nào có kết nối internet. Dễ sử dụng.	Ít an toàn hơn. Có thể bị hack hoặc bị xâm nhập.	Người cần truy cập ví thường xuyên và không có nhiều tiền để lưu trữ.
Ví di động	Một loại ví được cài đặt trên thiết bị di động.	Tiện lợi. Có thể truy cập từ bất kỳ đâu.	Có thể bị mất nếu thiết bị bị thất lạc, bị đánh cắp hoặc bị hack.	Người cần thực hiện giao dịch khi di chuyển và không có nhiều tiền để lưu trữ.
Ví máy tính để bàn	Một loại ví được cài đặt trên máy tính để bàn.	An toàn hơn ví trực tuyến. Có thể sử dụng khi không kết nối mạng.	Có thể bị hack nếu máy tính bị nhiễm phần mềm độc hại.	Người muốn lưu trữ lượng lớn bitcoin và thoải mái sử dụng máy tính để bàn.
Ví cứng	Một thiết bị vật lý lưu trữ bitcoin ngoại tuyến.	Rất an toàn. Có thể sử dụng khi không kết nối mạng.	Tiền có thể không lấy lại được nếu thiết bị bị mất hoặc bị đánh cắp.	Người muốn lưu trữ lượng lớn bitcoin và sẵn sàng chi trả để có thêm sự an toàn từ ví cứng.
Ví giấy	Bản ghi vật lý của khóa riêng và khóa công khai của ví Bitcoin.	Rất an toàn. Có thể sử dụng khi không kết nối mạng.	Có thể bị mất hoặc bị đánh cắp nếu bản ghi vật lý bị thất lạc hoặc bị lấy cắp.	Người muốn lưu trữ lượng lớn bitcoin và sẵn sàng thực hiện các biện pháp phòng ngừa bổ sung để đảm bảo tính an toàn.

Vì các khóa có thể được chuyển từ thiết bị này sang thiết bị khác, “tình trạng” của ví Bitcoin của bạn không cố định. Ví dụ, nếu tôi tạo khóa ví Bitcoin trên máy tính và sau đó tải chúng lên điện thoại, thì “ví máy tính để bàn” sẽ trở thành “ví di động.”



Khi lưu trữ bitcoin, không chỉ là vấn đề ai kiểm soát chúng — còn có nhiều rủi ro khác cần cân nhắc. Chính vì vậy, việc tìm một giải pháp lưu trữ an toàn vừa tiện lợi là rất quan trọng.

Khi phân tích các điểm cộng và điểm trừ của các loại ví khác nhau, bạn sẽ nhận ra rằng không có loại ví nào hoàn hảo để đáp ứng tất cả các nhu cầu.

Khi chọn ví Bitcoin, bạn nên cân nhắc một số yếu tố sau:

-  **Bảo mật:** Đảm bảo ví có các biện pháp bảo mật mạnh như xác thực hai yếu tố và chính sách mật khẩu an toàn.
-  **Quyền riêng tư:** Xem xét liệu ví có cho phép bạn ẩn danh hay yêu cầu thông tin cá nhân để tạo tài khoản.
-  **Dễ sử dụng:** Chọn ví dễ sử dụng và dễ điều hướng, đặc biệt nếu bạn mới làm quen với Bitcoin.
-  **Tương thích:** Đảm bảo ví tương thích với thiết bị và hệ điều hành của bạn.
-  **Phí:** So sánh các khoản phí của các loại ví khác nhau để đảm bảo bạn nhận được mức phí tốt nhất.
-  **Uy tín:** Tìm hiểu về uy tín của ví và nhóm phát triển để đảm bảo tính đáng tin cậy.
-  **Quyền kiểm soát:** Một số ví cho phép bạn kiểm soát nhiều hơn đối với khóa riêng, đây có thể là lợi thế về bảo mật.

Hãy cân nhắc liệu bạn muốn một loại ví cho phép bạn toàn quyền kiểm soát hay một loại ví thân thiện với người dùng hơn nhưng có thể hạn chế quyền kiểm soát.

7.2.3 Mã nguồn mở và mã nguồn đóng

Một yếu tố quan trọng khác cần lưu ý khi chọn ví Bitcoin là liệu ứng dụng hoặc phần mềm đó có mã nguồn mở hay không.

Mã nguồn mở rất quan trọng vì nó cho phép cộng đồng kiểm tra mã và tiếp tục phát triển dự án nếu nhóm phát triển ngừng làm việc.

Cách sử dụng Bitcoin



Cũng giống như mã nguồn của Bitcoin hoàn toàn mở để mọi người có thể kiểm tra, sử dụng và chỉnh sửa, mã nguồn của ví bạn dùng để lưu trữ bitcoin cũng nên được mở như vậy.

Hoạt động: Thảo luận trên lớp và đánh giá các ví Bitcoin trên bitcoin.org

Truy cập trang web sau: <https://bitcoin.org/en/choose-your-wallet> và sử dụng kiến thức mới học về các loại ví Bitcoin để chọn ra ví phù hợp nhất dựa trên các tiêu chí đã thảo luận hôm nay.

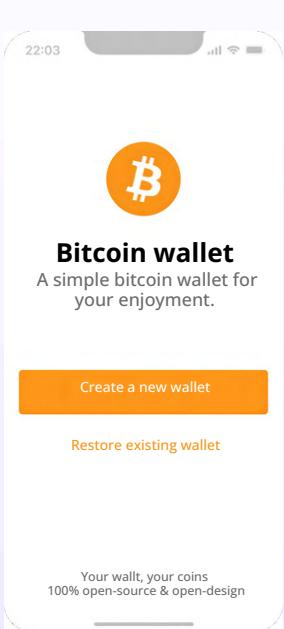


7.3 Thiết lập ví bitcoin di động

Bây giờ khi đã hiểu rõ hơn về các loại ví Bitcoin và sự khác biệt giữa chúng, chúng ta sẽ xem cách sử dụng một ví trên thực tế. Trong ví dụ này, chúng ta sẽ tạo một ví di động trực tiếp trên điện thoại thông minh.

Hoạt động: Thiết lập hoặc khôi phục ví Bitcoin

Nếu học sinh không có điện thoại di động, giáo viên sẽ cung cấp điện thoại để học sinh mượn. Hoạt động này có hai lựa chọn.



Bài tập trên lớp: Tùy chọn 1 — Tải về một ví mới.

Cách tạo và sử dụng ví Bitcoin:

- 1 Tim ứng dụng trên App Store (iOS) hoặc Google Play Store (Android).
- 2 Mở ứng dụng và nhập cụm từ khôi phục gồm 12 hoặc 24 từ của bạn (đôi khi còn được gọi là cụm từ seed). **Hãy chắc chắn rằng bạn đã ghi lại và cất giữ nó ở một nơi an toàn!** Cụm từ khôi phục này cho phép bạn khôi phục toàn quyền truy cập vào tài sản của mình nếu cần.
- 3 Tiếp theo, bạn phải xác nhận rằng mình đã thực sự lưu lại cụm từ khôi phục hoặc cụm từ seed. Để làm điều này, bạn cần nhập lại các từ trong cụm từ seed theo đúng thứ tự.
- 4 Để tăng cường bảo mật, một số ví cho phép bạn chọn mật khẩu an toàn. khóa riêng và địa chỉ Bitcoin đầu tiên được ví của bạn tự động tạo.

Your Seed Phrase

Your Seed Phrase is used to generate and recover your account.

- 1. issue 2. flame 3. sample
- 4. lyrics 5. find 6. vault
- 7. announce 8. banner 9. cute
- 10. damage 11. civil 12. goat

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.

Hãy coi khóa công khai của bạn như địa chỉ email — bạn muốn chia sẻ nó với người khác để họ có thể gửi bitcoin cho bạn — hoặc giống như khi chia sẻ địa chỉ email để nhận thư.

Hãy coi khóa riêng thì giống như mật khẩu email của bạn — bạn không bao giờ muốn chia sẻ nó với ai, vì điều đó sẽ cho họ quyền truy cập vào email của bạn.

- 5 Sử dụng địa chỉ "nhận" của bạn để nhận bitcoin. Chuyển bitcoin vào ví của bạn. Với ví tự lưu ký, bạn không phải lúc nào cũng có thể mua bitcoin trực tiếp bằng tiền pháp định, vì vậy bạn có thể cần mua và chuyển bitcoin từ sàn giao dịch trước.

Cách sử dụng Bitcoin

Bài tập trên lớp: Tùy chọn 2 – Khôi phục ví (Giới hạn thời gian).

Tải ví Bitcoin và nạp một ít satoshi vào mỗi ví học sinh.

Phát cho mỗi học sinh một tờ giấy chứa cụm từ seed để khôi phục ví.

Hướng dẫn học sinh từng bước:

- Khi bạn mở ví lần đầu, bạn sẽ thấy ba tùy chọn để tạo ví. Chạm vào **[Nhập ví hiện có]**. Sau đó, chạm vào **[Khôi phục bằng cụm từ khôi phục]** khi màn hình giới thiệu hiện ra.
- Nhập cụm từ khôi phục gồm 12, 18 hoặc 24 từ theo đúng thứ tự.
- Chạm vào **[Khôi phục]** để hoàn tất.
- Bạn sẽ thấy thông báo “Khôi phục thành công” khi ví đã được khôi phục.

7.4 Nhận và gửi giao dịch

Một giao dịch bitcoin là sự chuyển quyền sở hữu bitcoin hiện có sang một chủ sở hữu mới. Tuy nhiên, thay vì chuyển các đồng coin thực tế, tất cả các nút trong mạng sẽ cập nhật bản sao sổ cái công khai của riêng họ để phản ánh sự thay đổi quyền sở hữu này.

Khi gửi một giao dịch bitcoin, người gửi sẽ ký một thông điệp mà chỉ họ mới có thể ký bằng khóa riêng của mình, qua đó thông báo cho mạng rằng quyền sở hữu bitcoin đã được chuyển sang địa chỉ của người nhận.

Bitcoin bây giờ sẽ được liên kết với một địa chỉ mà chỉ chủ sở hữu mới có thể gửi đi, điều này mang lại cho họ quyền sở hữu các bitcoin đó.

SỔ CÁI

Chủ tài khoản	Giá trị
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,50
Robert	2,00
Eliana	1,75
Daniel	5,25

SỔ CÁI

Giao dịch Bitcoin
Tin nhắn yêu cầu
Jim gửi 0,50 BTC cho Eliana
Jim ▶ Eliana 0,50 BTC

Chủ tài khoản	Giá trị
Sam	2,50
Adam	3,00
Michael	6,00
Jim	1,50
Robert	2,00
Eliana	1,75
Daniel	5,25

Giao dịch Bitcoin mới được khởi tạo từ các ví trên toàn thế giới, nhưng không có một bộ xử lý thanh toán trung tâm nào. Thay vào đó, các thợ đào trên toàn cầu cạnh tranh để ghi lại các giao dịch vào sổ cái.

Giả sử Jim nợ Eliana 0,5 BTC và sẵn sàng trả cho cô ấy. Cả hai đều có ví điện tử.



- 1 Eliana chia sẻ địa chỉ ví của cô ấy với Jim.
- 2 Jim sử dụng phần mềm ví của mình để tạo giao dịch, bao gồm địa chỉ của Eliana, số tiền chuyển (0,5 BTC), và phí cho thợ đào.
- 3 Sau khi ký giao dịch, nó được phát sóng tới mạng lưới, nơi các nút kiểm tra và xác minh. Các nút kiểm tra tính hợp lệ của giao dịch và đảm bảo Jim có đủ số dư. Nếu không đủ, giao dịch sẽ bị từ chối ngay lập tức.
- 4 Khi giao dịch được xác minh, các thợ đào thêm giao dịch vào blockchain (blockchain) và số tiền được chuyển tới địa chỉ của Eliana.
- 5 Eliana sau đó có thể sử dụng khóa riêng của mình để truy cập số tiền đã chuyển trong ví của cô ấy.

Điều quan trọng cần lưu ý là khi giao dịch đã hoàn thành, nó không thể bị đảo ngược.

Cách một giao dịch Bitcoin hoạt động



Nhận Giao Dịch Bitcoin:



Để nhận bitcoin, bạn cần cung cấp địa chỉ ví Bitcoin của mình cho người gửi. Đây là một chuỗi ký tự gồm chữ và số duy nhất đại diện cho ví của bạn và được dùng để xác định ví đó trên mạng lưới Bitcoin. Bạn có thể tìm địa chỉ ví của mình bằng cách đăng nhập vào ví Bitcoin và tìm tùy chọn “Nhận” hoặc “Nạp” bitcoin.

Bạn có thể chia sẻ địa chỉ Bitcoin của mình với người gửi theo một trong các cách sau:

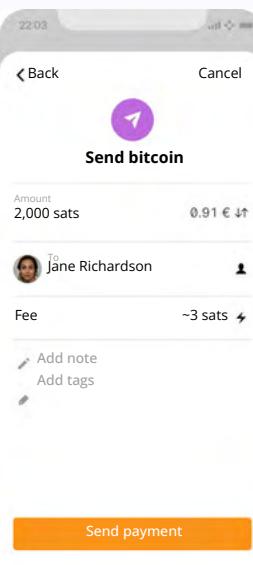
- 1 Sao chép và dán địa chỉ: Bạn có thể sao chép địa chỉ bằng cách bôi đen rồi nhấn “Sao chép” trên bàn phím, sau đó dán vào email hoặc tin nhắn gửi cho người gửi.
- 2 Chia sẻ một liên kết đến ví Bitcoin của bạn: Một số ví Bitcoin cho phép bạn tạo một liên kết đến ví của mình để chia sẻ với người gửi. Họ có thể nhấp vào liên kết đó để truy cập ví và gửi bitcoin cho bạn.
- 3 Chia sẻ mã QR: Nếu người gửi dùng điện thoại thông minh có ứng dụng ví Bitcoin, họ có thể quét mã QR để lấy địa chỉ Bitcoin của bạn.

Cách sử dụng Bitcoin

Khi người gửi đã có địa chỉ Bitcoin của bạn, họ có thể gửi bitcoin cho bạn bằng cách nhập địa chỉ của bạn và số lượng họ muốn gửi, rồi bắt đầu giao dịch. Bitcoin sau đó sẽ được chuyển đến ví của bạn và sẽ hiển thị khi giao dịch được xác nhận trên mạng lưới Bitcoin. Quá trình này thường mất vài phút.

Tiếp theo, chúng ta sẽ tìm hiểu cách gửi giao dịch bitcoin.

Gửi Giao Dịch Bitcoin:



Để gửi bitcoin, bạn cần một số thứ: ví Bitcoin, địa chỉ Bitcoin của người nhận và số lượng bitcoin bạn muốn gửi.

- Mở ví Bitcoin của bạn. Một mã SMS sẽ được gửi đến số điện thoại của bạn và bạn sẽ cần nhập mã này vào ô thoại. Ngoài ra, nếu bạn đã bật xác thực hai yếu tố (Google 2FA), bạn sẽ cần nhập mã sáu chữ số từ ứng dụng Google Authenticator.
- Điều hướng đến tính năng "Gửi" hoặc "Rút" và sao chép địa chỉ của người nhận.
- Nhập địa chỉ Bitcoin của người nhận bằng cách dán vào trường "Tới".
- Nhập số lượng bitcoin bạn muốn gửi vào trường "Số lượng".
- Kiểm tra kỹ lại địa chỉ người nhận và số lượng cần gửi.
- Trước khi nhấp vào "Xác nhận và Gửi", chúng tôi khuyên bạn nên kiểm tra lại thông tin giao dịch một lần nữa để đảm bảo bạn đang gửi đúng số lượng bitcoin đến đúng địa chỉ ví.
- Xác nhận giao dịch và chờ mạng lưới xác nhận giao dịch.

Giờ bạn đã biết cách đánh giá, lựa chọn và thiết lập một ví Bitcoin tự quản. Việc gửi bitcoin từ ví này sang ví khác trên mạng lưới Bitcoin được gọi là gửi một giao dịch "trên chuỗi" (on-chain). Điều này có nghĩa là giao dịch diễn ra trên blockchain chính của mạng lưới Bitcoin. Giao dịch trên chuỗi là cách an toàn nhất để thực hiện giao dịch bằng bitcoin. Tuy nhiên, các giao dịch trên chuỗi thường chậm hơn và có thể tốn kém đáng kể so với các tùy chọn khác, chẳng hạn như các giao dịch Lightning mà chúng ta sẽ tìm hiểu trong Chương 8.

Hoạt động: Giao dịch Bitcoin trong thực tế

Mục tiêu: Hiểu các khái niệm cốt lõi và cơ chế hoạt động của một giao dịch bitcoin ngang hàng

Trước khi bắt đầu, hãy cùng ôn lại nhanh những thành phần chính trong một giao dịch Bitcoin:

- Người gửi và người nhận là các bên muốn thực hiện giao dịch với nhau.
- Các nút (nodes) xác thực giao dịch và lưu trữ một bản sao đầy đủ của blockchain. Nút nhẹ (light nodes) cho phép người dùng xác thực giao dịch mà không cần sử dụng quá nhiều bộ nhớ và tài nguyên tính toán.
- Thợ đào chịu trách nhiệm thêm các giao dịch mới vào blockchain.

Hiểu vai trò của bạn. Bạn sẽ được giao một trong các vai trò sau: người gửi, người nhận, nút, hoặc thợ đào.

- ◆ Người gửi sẽ chịu trách nhiệm tạo và phát đi các giao dịch.
- ◆ Người nhận sẽ chịu trách nhiệm nhận và kiểm tra các giao dịch.
- ◆ Nút sẽ chịu trách nhiệm xác thực các giao dịch.
- ◆ Thợ đào sẽ chịu trách nhiệm thêm các giao dịch vào blockchain.

Cả nút và người nhận đều phải xác minh giao dịch

1 Với vai trò là người gửi: Tạo một giao dịch.

Để tạo một giao dịch, hãy làm theo các bước sau: Lấy một tờ ghi giao dịch và viết số lượng coin bạn muốn gửi cùng với tên hoặc chữ viết tắt của người nhận. Ký tên hoặc ghi chữ viết tắt của bạn lên tờ ghi này, mô phỏng việc sử dụng khóa riêng. Chuyển tờ ghi giao dịch cùng với số coin tương ứng cho người nhận.

2 Với vai trò là người nhận: Bạn có trách nhiệm xác minh các giao dịch. Hãy làm theo các bước sau:

- ◆ Kiểm tra tờ ghi giao dịch để đảm bảo rằng số lượng coin và tên hoặc chữ viết tắt của người nhận được ghi đúng.
- ◆ Đếm số coin nhận được và so sánh với số coin được ghi trên tờ ghi.
- ◆ Nếu số coin khớp, hãy đánh dấu vào ô phê duyệt. Nếu số coin không khớp hoặc bạn có nghi ngờ, hãy từ chối giao dịch.

Số coin được gửi	Người gửi	Chữ ký của người gửi	Người nhận	Ngày và Giờ	Phê duyệt của người nhận

3 Với vai trò là nút: Xác minh và xác thực các giao dịch. Bạn chịu trách nhiệm kiểm tra xem giao dịch có hợp lệ hay không.

- ◆ Xác minh rằng địa chỉ của người gửi và người nhận đều hợp lệ.
- ◆ Kiểm tra xem người gửi có đủ số dư để hoàn tất giao dịch và giao dịch không chi tiêu lại cùng một số coin.

Số coin được gửi	Người gửi	Chữ ký của người gửi	Người nhận	Ngày và Giờ	Phê duyệt của nút

Cách sử dụng Bitcoin

4 Với vai trò là thợ đào: Bạn chịu trách nhiệm thêm các giao dịch vào blockchain. Hãy làm theo các bước sau:

- Kiểm tra các giao dịch đã được người nhận phê duyệt và được các nút xác thực.
- Lắc xí ngầu và so sánh kết quả với thợ đào khác. Thợ đào có số nhỏ hơn sẽ thêm giao dịch vào blockchain.
- Vì thời gian, công sức và năng lượng bạn bỏ ra, bạn sẽ nhận được một điểm. Khi hoạt động kết thúc, thợ đào có nhiều điểm nhất sẽ thắng.

**Một khi giao dịch đã được thêm vào blockchain, nó không thể bị thay đổi hoặc đảo ngược.

5 Theo dõi số dư coin của bạn: Trong suốt hoạt động, hãy theo dõi số dư coin của bạn bằng cách đếm số coin có trong ví kỹ thuật số.

Số coin được gửi	Người gửi	Chữ ký của người gửi	Người nhận	Ngày và Giờ	Phê duyệt

6 Thảo luận các khái niệm đã học với cả lớp.

7.5 Tiết kiệm bằng Bitcoin

Bitcoin là một cách để bảo vệ tiền của bạn khỏi lạm phát và tránh bị kiểm soát bởi bất kỳ ai, nếu bạn sử dụng đúng cách. Tiết kiệm bằng Bitcoin mang đến một phương tiện để lưu trữ, tích lũy và xây dựng tài sản theo thời gian. Như bạn đã hiểu đến thời điểm này, loại tiền mà bạn chọn để tiết kiệm là một trong những quyết định quan trọng nhất mà bạn có thể đưa ra. Lựa chọn một cách khôn ngoan sẽ giúp bạn xây dựng một tương lai tốt đẹp hơn cho bản thân và gia đình.



An toàn: Khi được lưu trữ đúng cách, Bitcoin là hình thức tài sản duy nhất mà không ai có thể lấy đi khỏi bạn.

7.6 Đừng tin, hãy xác minh

Dù bạn làm gì với Bitcoin, hãy luôn ghi nhớ điều này: "Đừng tin, hãy xác minh." Trong Bitcoin không có người lãnh đạo. Bạn không nên tin mù quáng vào lời nói của bất kỳ ai. Thay vào đó, bạn nên luôn đặt câu hỏi với những gì bạn nghe và tự mình xác minh lại. Bằng cách làm theo nguyên tắc này, bạn sẽ bảo vệ bản thân khỏi nguy cơ mất bitcoin. Điều này áp dụng cho cả những tuyên bố như "Bitcoin tiếp theo," các "cơ hội đầu tư," hay lời hứa về "lợi nhuận nhanh chóng và dễ dàng."

Chương 7 đã trang bị cho bạn những kỹ năng quan trọng để sử dụng Bitcoin trong đời sống hằng ngày. Bạn đã học cách nhận và trao đổi bitcoin theo nhiều cách khác nhau, cũng như cách giữ chúng an toàn bằng các loại ví khác nhau.

Thông qua việc thiết lập ví Bitcoin trên điện thoại di động và thực hiện giao dịch với người khác, bạn đã có trải nghiệm thực tế để tự tin sử dụng Bitcoin mỗi ngày. Khi hiểu Bitcoin là một phương tiện để tiết kiệm và tuân theo nguyên tắc "Đừng tin, hãy xác minh," bạn đang nắm quyền kiểm soát tài chính của chính mình.

Trong chương tiếp theo, chúng ta sẽ tìm hiểu về Lightning Network. Chúng ta sẽ khám phá cách công nghệ đột phá này đang thay đổi cách mọi người trên toàn thế giới tiếp cận và sử dụng tiền. Từ các giao dịch hằng ngày đến những ứng dụng nâng cao hơn, bạn sẽ học cách Lightning Network trao quyền cho cá nhân, cộng đồng và doanh nghiệp bằng cách cung cấp quyền tiếp cận các dịch vụ tài chính.

Chương #8

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

8.0 Giới thiệu

Hoạt động: Xem “Giải thích Lightning Network của Bitcoin:
Cách nó hoạt động thực sự”

8.1 Lightning Network

8.2 Các loại ví Lightning khác nhau

8.2.1 Ví tự lưu ký và ví lưu ký

8.2.2 Mã nguồn mở và mã nguồn đóng

8.3 Thiết lập ví Lightning Bitcoin

8.4 Gửi và nhận giao dịch Lightning

Hoạt động: Cuộc đua tiếp sức ví Lightning

8.5 Mua cà phê và hàng tạp hóa bằng Bitcoin

8.5.1 Trực tuyến: Plugin thanh toán — Thương mại điện tử

8.5.2 Trực tiếp: Tìm thương nhân trong khu vực của bạn

8.5.3 Công cụ chuyển tiếp: Thẻ quà tặng và Thẻ thanh toán

8.5.4 Kinh tế tuần hoàn và Bitcoin như một phương tiện trao đổi

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

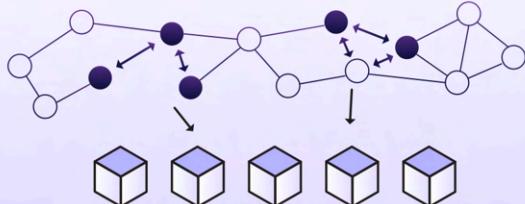
8.0 Giới thiệu

Chúng tôi đang xây dựng mạng lưới tương tự Visa cho Bitcoin. Nhưng điều tôi thấy mạnh mẽ là, không như Visa, bất kỳ ai cũng có thể phát triển trên nền tảng này.

Elizabeth Stark

Các công nghệ thường phát triển và mở rộng theo các lớp, giống như một ngăn xếp. Hãy nghĩ đến trang web, email, hoặc mạng xã hội yêu thích của bạn: chúng được xây dựng trên giao thức internet, giao thức này lại được xây dựng trên máy tính, còn máy tính được xây dựng dựa trên điện, và cứ như vậy. Những công nghệ này ban đầu có thiết kế rất đơn giản và sau đó liên tục được cải tiến theo thời gian.

Bitcoin cũng không ngoại lệ. Như Andreas Antonopoulos từng nói nổi tiếng, "Bitcoin là internet của tiền." Bitcoin chính là lớp nền tảng của tiên kỹ thuật số vững chắc, cung cấp nền tảng vững vàng để các công nghệ mới được xây dựng lên trên đó.

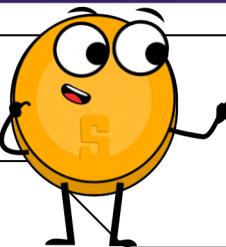


Một trong những lớp này được gọi là Lightning Network. Đây giống như một "đường cao tốc siêu nhanh" dành cho Bitcoin, giúp mọi người gửi và nhận bitcoin nhanh chóng với phí rất thấp. Lightning Network cho phép người dùng thực hiện các giao dịch nhỏ ngay lập tức trên nền tảng mạng Bitcoin thông thường. Điều này làm cho việc mua một tách cà phê hay trả tiền cho bạn bè trở nên đơn giản và nhanh chóng!

Hãy nhớ: Satoshi giống như đồng xu nhỏ nhất của Bitcoin. Giống như một đô la có thể chia ra thành xu, một bitcoin cũng có thể chia nhỏ thành các đơn vị gọi là satoshi. Một bitcoin bằng 100 triệu satoshi, khiến satoshi trở thành phần giá trị nhỏ nhất trong hệ thống Bitcoin. Trong chương này, khi chúng ta nói về việc gửi bitcoin qua Lightning Network, chúng ta sẽ gọi đó là "gửi sats," tức là những phần nhỏ hơn của một bitcoin.

Sats	Bitcoin
1	0,00000001
10	0,00000010
100	0,00000100
1.000	0,00001000
10.000	0,00010000
100.000	0,01000000
1.000.000	0,10000000
10.000.000	1,00000000
100.000.000	10,00000000

Hoạt động: Xem video này về Lightning Network



8.1 Lightning Network

Như chúng ta vừa thấy, Lightning Network hoạt động như một hệ thống thanh toán, giúp các giao dịch bằng bitcoin diễn ra nhanh chóng và tiết kiệm chi phí. Nó vận hành bằng cách thiết lập một ví chung, nơi cả hai bên đều giữ một số bitcoin. Hai bên có thể thực hiện nhiều giao dịch với nhau mà không cần ghi lại từng giao dịch trên sổ cái chính. Số dư cuối cùng sẽ được ghi vào sổ cái khi các giao dịch hoàn tất.



Lightning Network là một hệ thống thanh toán cho phép người dùng gửi và nhận tiền nhanh chóng và tiết kiệm chi phí bằng bitcoin. Nó hoạt động bằng cách thiết lập một ví chung, nơi cả hai người lưu trữ bitcoin của mình, sau đó thực hiện các giao dịch không giới hạn với nhau mà không ảnh hưởng đến blockchain chính. Khi hoàn tất, số dư cuối cùng sẽ được ghi lại trên blockchain chính.

Hãy tưởng tượng một ngày làm việc tại quán cà phê. Dự định ở lại cả ngày, bạn mở một tài khoản thanh toán và trả trước một số tiền thay vì trả mỗi lần gọi món. Khi kết thúc ngày làm việc và chuẩn bị ra về, bạn và chủ quán cùng xem lại tài khoản để thanh toán hóa đơn cuối cùng. Nếu bạn đã trả trước nhiều hơn tổng số tiền của hóa đơn, bạn sẽ được nhận lại phần tiền chưa sử dụng.

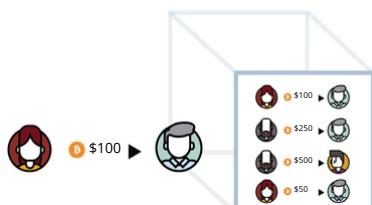
Bây giờ, hãy tưởng tượng hàng ngàn người cùng làm điều tương tự cùng một lúc và cho phép người khác sử dụng tài khoản thanh toán của họ để kết nối với nhiều người hơn. Đó chính là Lightning Network!

Với Lightning, bạn có thể gửi thanh toán cho bất kỳ ai trong mạng lưới, không chỉ người mà bạn trực tiếp chia sẻ tài khoản thanh toán. Thanh toán của bạn có thể đi qua nhiều điểm trong mạng cho đến khi đến được đích, ngay cả khi bạn không có kênh mở trực tiếp với người nhận.

Hãy cùng xem sự khác biệt giữa giao dịch trên chuỗi (giao dịch mà chúng ta đã bàn ở Chương 7) và giao dịch ngoài chuỗi (Lightning Network).

Giao dịch trên chuỗi:

Đây là các giao dịch diễn ra trực tiếp trên blockchain Bitcoin. Chúng mất khoảng 10 phút để được xác nhận, và phí giao dịch phụ thuộc vào kích thước giao dịch tính theo byte. Những giao dịch này bảo mật hơn nhưng chậm hơn.

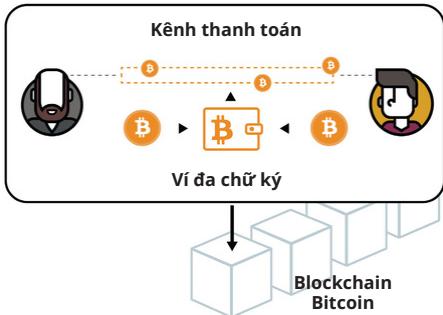


Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

Giao dịch ngoài chuỗi (Lightning Network):

Các giao dịch này diễn ra trên một mạng riêng biệt được xây dựng trên nền tảng blockchain Bitcoin. Chúng được xử lý nhanh hơn và có phí thấp hơn.

Loại giao dịch này thường được sử dụng ở những nơi có quy định và luật pháp hỗ trợ, cũng như nơi các yếu tố như tốc độ và chi phí giao dịch được ưu tiên hơn.



Mạng thanh toán	Mạng Bitcoin	Lightning Network
Định nghĩa	Một mạng kỹ thuật số phi tập trung sử dụng mật mã học để bảo mật các giao dịch tài chính.	Giao thức thanh toán lớp thứ hai hoạt động trên blockchain Bitcoin, cho phép giao dịch nhanh hơn và rẻ hơn.
Ưu điểm	Phi tập trung và an toàn. Không có việc hoàn tiền hoặc gian lận. Có thể sử dụng ẩn danh. Được chấp nhận trên toàn cầu.	Giao dịch nhanh hơn và phí thấp hơn. Khả năng mở rộng cao hơn. Giao dịch ngoài chuỗi không làm tắc nghẽn blockchain .
Nhược điểm	Thời gian giao dịch chậm. Phí cao đối với một số loại giao dịch nhất định. Phức tạp với người mới bắt đầu.	Cần tin tưởng vào người vận hành kênh. Vẫn còn trong giai đoạn thử nghiệm và chưa được áp dụng rộng rãi. Cần thực hiện giao dịch trên chuỗi để mở và đóng kênh.

8.2 Các loại ví Lightning khác nhau

Ví Lightning hơi khác với ví Bitcoin, mặc dù chức năng chính của cả hai đều là nhận và gửi bitcoin. Điểm khác biệt là ví Lightning cho phép bạn gửi bitcoin trên Lightning Network, vốn là lớp thứ hai được xây dựng trên mạng lưới Bitcoin.

Cũng như chúng ta đã thấy ở chương trước với ví Bitcoin, ví Lightning cũng có những đặc điểm khác nhau mà bạn cần cân nhắc trước khi chọn sử dụng.

8.2.1 Ví tự lưu ký và ví lưu ký

Ví Lightning có thể được chia thành nhiều loại rất cụ thể, nhưng để đơn giản, chúng ta sẽ chia thành hai loại: ví tự lưu ký và ví lưu ký.

Giống như ví Bitcoin, ví Lightning tự lưu ký là ví mà bạn kiểm soát các khóa riêng của ví, trong khi ví Lightning lưu ký là ví mà người khác kiểm soát các khóa đó.

Khi sử dụng ví lưu ký, bạn chỉ được quyền truy cập vào ví nhưng phải phụ thuộc vào người khác để được phép sử dụng số tiền của mình; bạn đang đánh đổi quyền sở hữu tiền để lấy sự tiện lợi.

Điều này có thể chấp nhận được đối với số tiền nhỏ, mặc dù khi đã hiểu rõ về công nghệ, bạn nên sử dụng ví tự lưu ký.

Trong phần tiếp theo, chúng ta sẽ chỉ nói về ví Lightning tự lưu ký.

8.2.2 Mã nguồn mở và mã nguồn đóng

Cũng giống như ví Bitcoin mà chúng ta đã thấy trong chương trước, ví Lightning có thể là mã nguồn mở hoặc mã nguồn đóng. Luôn sử dụng ví mã nguồn mở vì chúng hoàn toàn minh bạch, được công đồng xem xét và kiểm duyệt kỹ càng.

Một ứng dụng mã nguồn mở còn có nghĩa là bất kỳ ai cũng có thể đóng góp để cải thiện phần mềm, giúp nó trở thành lựa chọn tốt hơn cho người dùng.

8.3 Thiết lập ví Lightning Bitcoin

Thiết lập ví Bitcoin Lightning tự lưu ký cũng giống như thiết lập ví Bitcoin tự lưu ký trên chuỗi chính.

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

Bài tập trên lớp — Lựa chọn 1: Tải xuống một ví Lightning tự lưu ký mới

Cách Tạo và Sử Dụng Ví Bitcoin Lightning

- 1** Tim ứng dụng trên App Store (iOS) hoặc Google Play Store (Android).
- 2** Mở ứng dụng và nhập cụm từ khôi phục gồm 12 hoặc 24 từ của bạn (đôi khi còn được gọi là cụm từ seed). **Hãy chắc chắn rằng bạn đã ghi lại và cất giữ nó ở một nơi an toàn!** Cụm từ khôi phục này cho phép bạn khôi phục toàn quyền truy cập vào tài sản của mình nếu cần.

Hãy nhớ rằng nếu bạn làm mất hoặc quên chuỗi từ này, bạn sẽ không thể truy cập vào số bitcoin của mình nếu mất quyền truy cập vào ví.
- 3** Tiếp theo, bạn phải xác nhận rằng mình đã thực sự lưu lại cụm từ khôi phục hoặc cụm từ seed. Để làm điều này, bạn cần nhập lại các từ trong cụm từ seed theo đúng thứ tự.
- 4** Để tăng cường bảo mật, một số ví cho phép bạn chọn mật khẩu an toàn. khóa riêng và địa chỉ Bitcoin đầu tiên được ví của bạn tự động tạo.
- 5** Tạo hóa đơn Lightning, địa chỉ hoặc mã QR để nhận bitcoin. Chuyển bitcoin vào ví của bạn. Với ví tự lưu ký, bạn không phải lúc nào cũng có thể mua bitcoin trực tiếp bằng tiền pháp định, nên có thể bạn cần mua và chuyển bitcoin từ sàn giao dịch trước.

Cụm từ seed của bạn

Cụm từ seed được sử dụng để tạo và khôi phục tài khoản của bạn.

- | | | | | |
|----------|------------|----------|----------|-----------|
| 1 Issue | 2 Flame | 3 Sample | 4 Lyrics | 5 Find |
| 6 Vault | 7 Scissors | 8 Banner | 9 Cute | 10 Damage |
| 11 Civil | 12 Goat | | | |

Vui lòng ghi lại 12 từ này trên một tờ giấy. Thứ tự các từ rất quan trọng. Seed phrase này sẽ giúp bạn khôi phục lại tài khoản khi cần thiết.

*Lưu ý: Nếu bạn sử dụng ví lưu ký, bạn sẽ không cần thực hiện một số bước trong phần 8.3. Việc sử dụng ví lưu ký đi kèm với rủi ro, vì bạn sẽ không kiểm soát được khóa riêng, đồng nghĩa với việc bạn không kiểm soát được số tiền trong ví của mình.

Giờ đây, sau khi đã thiết lập ví Bitcoin Lightning, chúng ta sẽ tìm hiểu cách nhận và gửi giao dịch Lightning cũng như cách chúng khác với các giao dịch on-chain mà chúng ta đã gửi trong Chương 7.

8.4 Gửi và nhận giao dịch Lightning

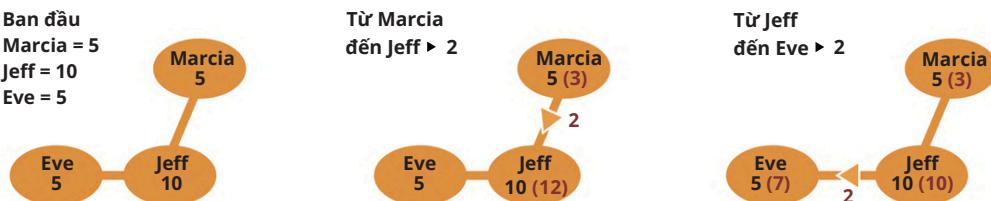
Với ví Lightning, việc sử dụng Bitcoin trở nên nhanh chóng, rẻ và riêng tư, giúp các giao dịch giữa hai người trở nên dễ dàng. Bạn có thể nhanh chóng gửi và nhận bitcoin cho các nhu cầu hằng ngày như mua cà phê hoặc đi mua sắm.

Hãy cùng xem một vài ví dụ về cách Lightning Network hoạt động trong thực tế.

Ví dụ 1:

Bên dưới, cả Marcia và Eve đều có 5 đơn vị tiền. Marcia muốn gửi 2 đơn vị của mình cho Eve, nên cô gửi 2 đơn vị đó cho Jeff. Jeff sau đó chuyển tiếp 2 đơn vị cho Eve, và bây giờ Eve có 7 đơn vị. Marcia hiện còn lại 3 đơn vị. Và thế là xong! Giao dịch đã hoàn tất.

Điểm mấu chốt ở đây là Marcia và Eve không cần phải thông qua ngân hàng hay bên trung gian nào khác để thực hiện giao dịch này.



Jeff đóng vai trò là một bên trung gian, hay còn gọi là “bên thứ ba đáng tin cậy” trong tình huống này, nơi Marcia và Eve không tin tưởng trực tiếp lẫn nhau. Jeff nhận 2 đơn vị tiền từ Marcia rồi chuyển lại cho Eve, hoàn tất giao dịch. Bằng cách sử dụng Jeff làm trung gian, Marcia và Eve có thể thực hiện giao dịch mà không cần đến ngân hàng hay tổ chức tập trung nào, giúp giao dịch nhanh hơn, rẻ hơn và an toàn hơn. Jeff là một yếu tố then chốt trong quá trình giao dịch ngang hàng này.

Là một người vận hành nút (node) trong giao dịch Lightning Network, Jeff nhận được một số lợi ích như sau:

Phí giao dịch

1 Jeff kiếm được một khoản phí nhỏ cho mỗi giao dịch đi qua nút của mình. Khoản phí này giúp bù đắp cho thời gian và công sức mà Jeff bỏ ra để duy trì và vận hành nút Lightning.

Tham gia mạng lưới

Bằng cách vận hành một nút Lightning, Jeff đang tham gia vào mạng lưới và góp phần tăng cường tính phi tập trung, bảo mật và ổn định cho hệ thống. Điều này giúp nâng cao uy tín và độ tin cậy của Jeff với tư cách là một người vận hành nút đáng tin cậy, khiến anh trở thành một trung gian hấp dẫn hơn cho các giao dịch trong tương lai.

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

3

Tăng trưởng mạng lưới

Khi Lightning Network phát triển và ngày càng có nhiều người sử dụng, số lượng giao dịch đi qua nút của Jeff có khả năng sẽ tăng lên. Điều này có thể mang lại thu nhập cao hơn từ phí giao dịch.

4

Tăng cường bảo mật mạng lưới

Vai trò trung gian của Jeff giúp tăng cường bảo mật cho mạng lưới bằng cách thêm một lớp bảo vệ giữa Marcia và Eve. Điều này có thể làm tăng sự tin tưởng của người dùng đối với mạng lưới, giúp thu hút người dùng mới và thúc đẩy sự phát triển. Tổng thể, việc vận hành một nút trong Lightning Network có thể mang lại cho Jeff nguồn thu nhập ổn định, đồng thời tạo cơ hội để anh đóng góp vào sự phát triển và mở rộng của mạng lưới.

Tóm lại, **các giao dịch trên chuỗi chậm hơn nhưng an toàn hơn, trong khi các giao dịch ngoài chuỗi (Lightning Network) nhanh hơn nhưng kém an toàn hơn**. Bạn nên cân nhắc sự đánh đổi giữa bảo mật và tốc độ tùy theo nhu cầu của mình.

Ví dụ 2:

Mina cực kỳ yêu thích McDonald's. Ngày nào cô ấy cũng đến đó ăn sáng, trưa và tối. Nhưng với quá nhiều phương thức thanh toán khác nhau, cô ấy không chắc nên chọn cách nào là tốt nhất. May mắn thay, Mina đã tìm hiểu một chút về Bitcoin và Lightning Network. Sau khi so sánh các bảng dưới đây, Mina hoàn toàn tin rằng sử dụng phương thức thanh toán Lightning là lựa chọn tối ưu.

Lightning Network và Hệ thống Ngân hàng Truyền thống

Lợi ích	Lightning	Hệ thống Ngân hàng Truyền thống
Tốc độ	Nhanh	Chậm
Minh bạch	Minh bạch	Không minh bạch
Bảo mật	An toàn	Dễ bị tấn công
Phí giao dịch	Thấp	Cao
Hòm nháp tài chính	Cao	Hạn chế

Lợi ích	Lightning	Hệ thống Ngân hàng Truyền thống
Khả năng mở rộng	Cao	Thấp
Quyền riêng tư	Cao	Trung bình
Khả năng tương tác	Cao	Thấp
Tuân thủ pháp lý	Trung bình	Cao
Hiệu quả chi phí	Cao	Trung bình

Visa, Inc.



Trung bình 1.700 giao dịch mỗi giây.

Khả năng xử lý lên đến 65.000 giao dịch mỗi giây.

Bitcoin trên chuỗi



Khả năng xử lý 7 giao dịch mỗi giây.

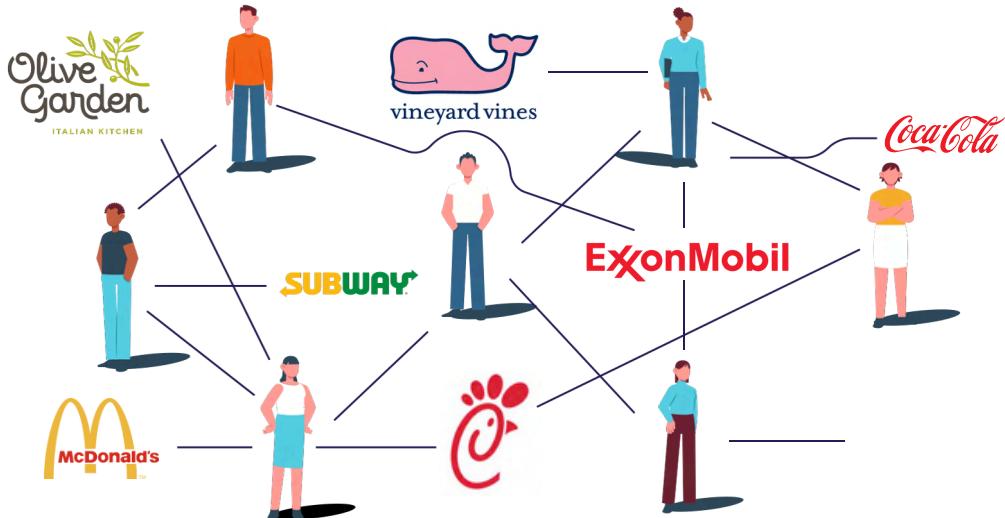
Bitcoin Lightning Network



Hàng triệu giao dịch mỗi giây.

Mina cũng rất thích các giao dịch nhanh, an toàn và tiết kiệm chi phí, vì vậy cô ấy quyết định sử dụng Lightning để thanh toán tại McDonald's. Với Lightning, cô ấy có thể tận hưởng bữa ăn của mình hơn nữa khi biết rằng các khoản thanh toán được xử lý ngay lập tức, an toàn và với phí thấp.Thêm vào đó, vì Lightning Network cung cấp sự bao gồm tài chính, Mina có thể thanh toán cho bữa ăn ngay cả khi cô ấy ở khu vực xa xôi tại El Salvador.

Để bắt đầu với Lightning, Mina trước tiên tải về một ví Lightning trên điện thoại của mình. Cô ấy sau đó nạp tiền vào ví bằng cách gửi một số bitcoin từ ví Bitcoin thường dùng sang ví Lightning mới này. Quá trình này được gọi là "nạp tiền vào ví" hoặc "nạp tiền vào kênh thanh toán." Mina có thể nạp vào ví bất kỳ số bitcoin nào cô ấy thấy thoải mái, nhưng cần lưu ý rằng số bitcoin bị khóa trong ví Lightning sẽ không thể dùng cho các giao dịch trên chuỗi của cô ấy.



Khi ví Lightning của Mina đã được nạp tiền, cô ấy có thể dùng nó để thanh toán tại McDonald's.

McDonald's có một nút Lightning, nên Mina có thể mở một kênh thanh toán với họ bằng cách gửi một số bitcoin từ ví Lightning của mình tới địa chỉ cụ thể do McDonald's cung cấp. Việc này chuyển bitcoin của cô ấy từ blockchain Bitcoin sang giao dịch ngoài chuỗi trên Lightning Network.

Với kênh thanh toán đã mở, Mina giờ có thể mua đồ tại McDonald's mà không cần phải mở kênh mới hay trả phí cao mỗi lần. Kênh sẽ giữ mở miễn là Mina và McDonald's đều muốn sử dụng nó. Ví dụ, nếu Mina mua một chiếc hamburger với giá 0,0005 bitcoin, kênh sẽ theo dõi rằng Mina còn 0,9995 bitcoin. Và nếu ngày hôm sau cô ấy mua một ly milkshake với giá 0,0003 bitcoin, kênh sẽ theo dõi rằng Mina còn 0,9992 bitcoin.

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

Khi Mina quyết định muốn dùng số bitcoin của mình cho việc khác, cô đóng kênh bằng cách phát hành một giao dịch đóng lên blockchain Bitcoin. Việc này được thực hiện bằng cách khởi tạo giao dịch đóng trong ví Lightning của cô, và giao dịch này chứa số dư cuối cùng của kênh được cả hai bên đồng ý. Giao dịch sau đó được phát lên blockchain Bitcoin và được thợ đào xác nhận. Khi giao dịch được xác nhận, kênh sẽ đóng lại, và số bitcoin còn lại trong kênh sẽ được trả lại cho Mina và McDonald's.

Cần lưu ý rằng việc đóng kênh có thể mất một thời gian để được xác nhận trên blockchain. Trong thời gian chờ đợi này, số tiền vẫn bị khóa trong kênh và không thể sử dụng cho các giao dịch trên chuỗi. Mina sẽ nhận được thông báo khi giao dịch đóng được xác nhận.

Giờ đây, khi đã thiết lập ví Lightning và hiểu cách sử dụng Lightning Network để gửi giao dịch, chúng ta sẽ chơi một trò chơi gửi satoshi (đơn vị nhỏ nhất của bitcoin) đến các bạn học trong lớp qua Lightning Network.



Đây là bản đồ toàn thế giới. Với Lightning Network, bạn có thể gửi satoshi đến bất kỳ người dùng nào có ví Bitcoin Lightning. Thanh toán sẽ đến trong vài giây và chỉ mất vài xu phí.

Hãy tự trải nghiệm nhé:



Hoạt động: Bài tập trên lớp - Cuộc đua tiếp sức ví Lightning

- 1** Đầu tiên, bạn cần tải xuống một ví Lightning trên điện thoại hoặc máy tính của mình.
- 2** Làm theo hướng dẫn cài đặt ví trên thiết bị trong Mục 8.3 của chương này.
- 3** Khi ví đã được cài đặt, mở ví lên và làm theo các bước hướng dẫn để thiết lập. Quá trình này có thể bao gồm việc tạo ví mới hoặc khôi phục ví đã có, đồng thời bảo mật ví bằng mật khẩu hoặc hình thức xác thực khác.
- 4** Tạo hóa đơn Lightning, địa chỉ, hoặc mã QR để nhận bitcoin.
- 5** Khi ví đã được thiết lập và bạn sẵn sàng nhận satoshi, giáo viên sẽ gửi cho bạn và nhóm một số satoshi khởi đầu trực tiếp vào ví của bạn.



- A** Mục tiêu của nhóm bạn là chuyển satoshi từ ví của người này sang người khác qua Lightning Network cho đến khi đến được người cuối cùng trong nhóm.
- B** Để gửi satoshi cho người khác, hãy mở ví của bạn và làm theo hướng dẫn để thực hiện thanh toán. Bạn sẽ cần cung cấp hóa đơn Lightning của người nhận hoặc quét mã QR và nhập số lượng satoshi muốn gửi.
- C** Nếu nhóm bạn là nhóm đầu tiên chuyển satoshi thành công đến người cuối cùng, các bạn sẽ chiến thắng! (Và được giữ số sats đó).

Thảo luận về bất kỳ khó khăn nào mà nhóm bạn gặp phải trong hoạt động này. Việc gửi giao dịch có dễ dàng, nhanh chóng và chi phí thấp không? Bạn có nghĩ rằng Lightning Network dễ sử dụng và dễ hiểu không?

Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

8.5 Mua cà phê và hàng tạp hóa bằng Bitcoin

Bạn đã bao giờ tự hỏi liệu mình có thể dùng bitcoin để mua ly cà phê mỗi ngày hay tích trữ hàng tạp hóa chưa? Hóa ra là hoàn toàn có thể. Hiện nay có nhiều lựa chọn, cả trực tuyến lẫn trực tiếp, cho phép bạn thanh toán bằng bitcoin. Chúng ta sẽ cùng khám phá một số lựa chọn đó cũng như các công cụ giúp bạn tìm cửa hàng địa phương chấp nhận bitcoin để chi tiêu.

Mặc dù việc thanh toán bằng thẻ tín dụng hay ứng dụng có vẻ đơn giản đối với người dùng, nhưng quá trình xử lý thanh toán thực chất rất phức tạp và liên quan đến nhiều bên khác nhau.

Quy trình xử lý thanh toán hoạt động như thế nào



Khi bạn mua hàng, có rất nhiều bên tham gia vào quá trình thanh toán, và mỗi bên đều tính một khoản phí. Đối với chủ cửa hàng, những khoản phí này có thể rất đáng kể — hơn 3% giá trị sản phẩm, là một con số lớn đối với họ. Đó là chưa kể đến phí chuyển đổi ngoại tệ!

Phí Xử Lý Thẻ Tín Dụng



Với Bitcoin và Lightning Network, các doanh nghiệp có thể nhận thanh toán ngay lập tức từ khắp nơi trên thế giới thông qua một hệ thống tiền tệ mở, an toàn, bản địa internet, không biên giới và chống kiểm duyệt.

Tiếp theo, chúng ta sẽ cùng tìm hiểu một số cách mà các thương nhân có thể dễ dàng chấp nhận thanh toán bằng bitcoin.

8.5.1 Trực tuyến: Plugin thanh toán — Thương mại điện tử

BTCPay Server là một trình xử lý thanh toán mã nguồn mở cho phép các thương nhân chấp nhận thanh toán bằng bitcoin mà không cần nhiều kiến thức kỹ thuật. Nó hoàn toàn miễn phí và không thu bất kỳ khoản phí hoa hồng nào.

Các doanh nghiệp trực tuyến có thể tích hợp BTCPay Server một cách dễ dàng bằng cách thêm plugin BTCPay vào trang web của mình.

Trở thành người xử lý thanh toán của chính bạn.



Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

Vì BTCPay Server là một dự án mã nguồn mở, không phải là một công ty, bạn có thể đóng góp cho dự án khi bạn tìm hiểu thêm về nó và lập trình máy tính.

Hãy truy cập trang web BTCPay Server tại <https://btcpayserver.org/> để biết thêm thông tin về cách sử dụng hệ thống thanh toán này cho cửa hàng trực tiếp hoặc kinh doanh trực tuyến của bạn.

The infographic highlights four key features of BTCPay Server:

- Miễn phí và mã nguồn mở**: Shows a hand holding a flower. Text: Miễn phí hoàn toàn theo giấy phép MIT. Không có phí giao dịch, đăng ký hay xử lý nào. Mã nguồn hoàn toàn mở. Thành toán trực tiếp, ngang hàng.
- Phi tập trung**: Shows a network graph. Text: Bất kỳ ai cũng có thể triển khai một máy chủ. Hãy trở thành bộ xử lý thanh toán tự lưu trữ và nhận thanh toán trực tiếp vào ví của bạn. Giúp bạn bè hoặc cộng đồng của bạn xử lý thanh toán cho họ. Một số lượng cửa hàng không giới hạn có thể được kết nối với cùng một máy chủ BTCPay Server.
- Độc lập, không qua bên trung gian**: Shows two people with a red slash through them. Text: Các bên thứ ba đáng tin cậy lại là điểm yếu về bảo mật. BTCPay loại bỏ hoàn toàn điều đó. Thành toán diễn ra trực tiếp theo mô hình ngang hàng. Dữ liệu không bị chia sẻ. Không có quy trình KYC (Xác minh danh tính) hay AML (Chống rửa tiền).
- An toàn**: Shows a padlock with a Bitcoin logo. Text: Khóa riêng của bạn không bao giờ bị yêu cầu. BTCPay tự lưu ký chỉ cần xpubkey (khôc công khai) để tạo hóa đơn. Mã nguồn mở và có thể được các chuyên gia bảo mật cùng lập trình viên kiểm tra.

Small text at the bottom right: con credits: No Mediator by Arthur Shain; decentralized by Silvia Santos from Noun Project

8.5.2 Trực tiếp: Tìm thương nhân trong khu vực của bạn

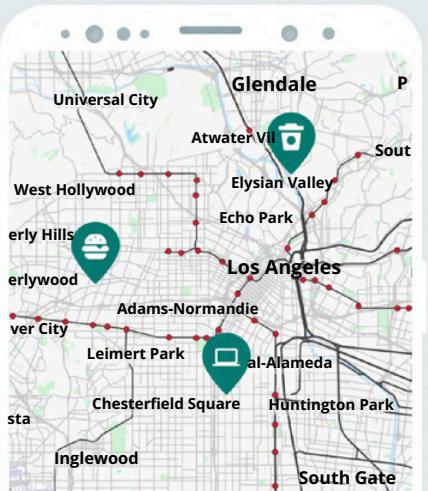
Các cửa hàng vật lý cũng có thể sử dụng BTCPay Server để chấp nhận thanh toán, hoặc đơn giản là tải ví Bitcoin về và nhận thanh toán Bitcoin trực tiếp từ điện thoại.



Để tìm thương nhân chấp nhận Bitcoin trong khu vực của bạn, hãy truy cập BTCTMap.org và tìm kiếm vùng của bạn. BTCTMap.org là bản đồ mã nguồn mở, nơi các thương nhân chấp nhận Bitcoin có thể đăng ký doanh nghiệp của họ. Đây là công cụ hữu ích cho những người muốn sử dụng bitcoin để thanh toán.


BTCMap.org

Easily find places to spend sats anywhere on the planet.



8.5.3 Công cụ chuyển tiếp: Phiếu mua hàng, thẻ quà tặng và thẻ thanh toán

Để mua sản phẩm hoặc dịch vụ từ các doanh nghiệp chưa chấp nhận Bitcoin, bạn có thể sử dụng một công cụ trung gian: thẻ quà tặng.

Một số doanh nghiệp chuyên mua bán thẻ quà tặng đổi lấy bitcoin. Điều này có nghĩa là bạn có thể mua thẻ quà tặng cho cửa hàng mình muốn đến bằng bitcoin và sau đó dùng thẻ quà tặng đó để thanh toán trực tiếp tại cửa hàng.

Vé máy bay, khách sạn, trò chơi, thẻ SIM... bạn có thể mua hầu như bất cứ thứ gì bằng bitcoin và thẻ quà tặng!

8.5.4 Kinh tế tuần hoàn và Bitcoin như một phương tiện trao đổi

Khái niệm kinh tế tuần hoàn bắt nguồn từ ý tưởng giảm thiểu lãng phí trong nền kinh tế bằng cách tái sử dụng và tái chế tối đa các sản phẩm và phụ phẩm.

Dựa trên khái niệm này, kinh tế tuần hoàn Bitcoin là một mô hình trong đó các giao dịch được thực hiện bằng bitcoin, và giá trị dưới dạng bitcoin được giữ lại và phát triển trong nền kinh tế, mang lại lợi ích cho cá nhân và doanh nghiệp.



Lightning Network: Sử dụng Bitcoin trong đời sống hàng ngày

Lightning Network cho phép các nền kinh tế tuần hoàn Bitcoin phát triển trên toàn thế giới nhờ các giao dịch bitcoin gần như tức thì và với phí cực thấp.



Nền kinh tế tuần hoàn Bitcoin đầu tiên từng được tạo ra nằm ở Arnhem, Hà Lan. Nó được hình thành từ trước khi Lightning Network ra đời, nhưng vào thời điểm đó, phí giao dịch trên chuỗi (on-chain) vẫn còn rất thấp!

KINH TẾ TUẦN HOÀN BITCOIN

VỤ NỔ LỚN

2013

 Arnhem-Nijmegen

Follow the project:

Nền kinh tế tuần hoàn thứ hai là Bitcoin Beach, tọa lạc tại El Zonte, El Salvador. Dự án này tận dụng sức mạnh của Lightning Network để mang lại khả năng thanh toán kỹ thuật số tức thì cho cộng đồng, phần lớn là người không có tài khoản ngân hàng, thông qua điện thoại thông minh.

Ngày nay, hàng trăm nền kinh tế tuần hoàn đang được xây dựng trên khắp thế giới, được thúc đẩy bởi Bitcoin, Lightning Network và các tài nguyên giáo dục.



Trên BTCMap.org, bạn cũng có thể tìm các cộng đồng Bitcoin, nơi bạn sẽ gặp gỡ những người dùng Bitcoin khác và tìm thấy các doanh nghiệp chấp nhận Bitcoin. Một số giáo viên và học viên của chúng tôi đã thêm doanh nghiệp và các nền kinh tế tuân hoà vào BTCMap.org, và khi bạn sẵn sàng, bạn cũng có thể làm điều đó!



Easily find places to spend sats anywhere on the planet.



Tài nguyên: btcmap.org/communities

Kết thúc Chương 8, bạn đã hiểu thêm về cách sử dụng Bitcoin trong đời sống hằng ngày thông qua Lightning Network. Lightning Network giúp giao dịch nhanh hơn, dễ tiếp cận hơn và mang đến cái nhìn sơ lược về cách Bitcoin sẽ tiếp tục phát triển theo từng lớp.

Trong Chương 9, chúng ta sẽ tìm hiểu khía cạnh kỹ thuật của Bitcoin. Từ mật mã học, nút, thợ đào và nhiều yếu tố khác, hãy sẵn sàng khám phá sâu hơn cách Bitcoin thật sự vận hành.

Chương #9

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.0 Giới thiệu

Hoạt động: Xem “Cách Bitcoin hoạt động bên trong”

9.1 Khóa công khai và khóa riêng: Bảo mật thông qua mật mã học

9.1.1 Mật mã học khóa công khai và khóa riêng

9.1.2 Giải thích hàm băm

Hoạt động: Tạo mã băm SHA-256

9.2 Mô hình UTXO

9.3 Nhìn kỹ hơn vào các nút Bitcoin và thợ đào

9.3.1 Nút Bitcoin là gì và cách làm thế nào để thiết lập một nút?

Hoạt động: Xem video về các nút Bitcoin

9.3.2 Thợ đào Bitcoin là gì và quá trình đào hoạt động như thế nào?

9.4 Mempool là gì?

Hoạt động: Mempool

9.5 Quy trình hoạt động của một giao dịch Bitcoin từ đầu đến cuối

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.0 Giới thiệu

Bitcoin không phải là “phi điều tiết”; nó được điều tiết bằng thuật toán thay vì bởi các cơ quan hành chính của chính phủ. Không bị tha hóa.

Andreas M. Antonopoulos

Trong chương này, chúng ta sẽ cùng tìm hiểu sâu hơn về công nghệ cho phép mạng lưới Bitcoin hoạt động một cách hoàn toàn phi tập trung. Chúng tôi sẽ giải thích bằng những thuật ngữ đơn giản về những gì xảy ra khi bạn gửi một giao dịch Bitcoin, cách các giao dịch đó được xử lý, và vai trò của thợ đào và các nút mạng trong hệ thống Bitcoin. Chúng ta sẽ đề cập đến một số khái niệm mang tính kỹ thuật và có phần thách thức trong chương này. Tuy nhiên, có một điều quan trọng cần ghi nhớ: rất nhiều người không hiểu cách Internet hoạt động, nhưng họ vẫn có thể sử dụng nó hàng ngày để gửi email, liên lạc với bạn bè qua mạng xã hội và thậm chí thanh toán hóa đơn. Việc tìm hiểu khía cạnh kỹ thuật của cách Bitcoin hoạt động là một hành trình dài mà không phải ai cũng muốn theo đuổi, ngay cả khi họ quyết định sử dụng nó như một loại tiền tệ. Mặc dù chúng tôi khuyến khích bạn tiếp tục học hỏi về mặt kỹ thuật của Bitcoin, chương này sẽ tập trung vào những khái niệm cơ bản và quan trọng nhất.

Cơ chế hoạt động của giao thức Bitcoin

Bằng chứng công việc



Dấu thời gian mật mã



Điều chỉnh độ khó



Kiến trúc mạng
ngang hàng



Hàm băm và cây
Merkle



Mật mã khóa
công khai



Giảm một
nửa trợ cấp
khối

Nếu bạn muốn hiểu sâu hơn về cách Bitcoin hoạt động từ góc độ kỹ thuật, chúng tôi đã cung cấp các tài liệu tham khảo ở phần cuối của cuốn sách này. Bạn cũng có thể đăng ký trên trang web của chúng tôi để nhận thông báo về Văn bằng Bitcoin - Phiên bản Kỹ thuật khi khóa học nâng cao này sẵn sàng.

Hãy bắt đầu bằng cách xem một video giới thiệu về cách mạng lưới Bitcoin vận hành.

Hoạt động: Xem
“Cách Bitcoin hoạt
động bên trong”



Như bạn đã thấy trong video, mạng lưới Bitcoin đơn giản chỉ là một sổ cái hoặc hồ sơ giao dịch được lưu trữ trên nhiều máy tính gọi là các nút. Sổ cái Bitcoin sử dụng bí danh, nghĩa là nó không chứa thông tin cá nhân mà chỉ ghi lại các giao dịch và địa chỉ. Sổ cái này hiển thị mọi bitcoin và các chuyển động của nó kể từ khi mạng lưới bắt đầu vào ngày 3 tháng 1 năm 2009.

Tiếp theo, chúng ta sẽ cùng tìm hiểu kỹ hơn về công nghệ giúp hệ thống này trở thành hiện thực.

9.1 Khóa công khai và khóa riêng: Bảo mật thông qua mật mã học

Điều mà Bitcoin mang lại cho chúng ta là một cam kết chắc chắn: chương trình sẽ thực thi chính xác như được chỉ định.

Andreas M. Antonopoulos

9.1.1 Mật mã học khóa công khai và khóa riêng

Mật mã học là một cách giữ bí mật thông tin bằng cách ngụy trang thông tin đó dưới dạng m



 Mã hóa là quá trình lấy thông tin và chuyển đổi nó thành một dạng mã đặc biệt, khiến cho bất kỳ ai không có phương pháp giải mã đúng không thể đọc được. Điều này giống như việc khóa một chiếc két sắt, chỉ có người có chìa khóa hoặc mật khẩu đúng mới mở được.

 Ngược lại, giải mã là quá trình lấy thông tin đã được mã hóa và biến nó trở lại dạng có thể đọc được, giống như mở khóa két sắt để có thể xem thông tin bên trong.

Chẳng hạn, giả sử John muốn gửi cho Arel một thông điệp bí mật mà không ai khác có thể đọc được. Họ đồng ý sử dụng phương pháp mã hóa Pigpen để biến đổi thông điệp trước khi gửi. Chỉ những người có chìa mã mới có thể giải mã được thông điệp, khiến nó không thể đọc được đối với người khác. Mặc dù phương pháp này ngày nay không được xem là an toàn, nhưng nó minh họa nguyên tắc của mã hóa khóa riêng để gửi thông điệp.

Cách giải

Mật mã Pigpen

Khi giải mật mã Pigpen, người chơi sẽ được cung cấp một thông điệp đã được mã hóa và một bảng mật mã. Để giải mã thông điệp, người chơi tìm ký hiệu trong thông điệp đã mã hóa trên bảng mật mã để xác định chữ cái tương ứng.

 Ví dụ về một thông điệp đã mã hóa:



A	B	C	J	.	K	L	S	W
D	E	F	M	.	N	F	T	X
G	H	I	P	.	Q	R	V	Z

Vậy, mã hóa hoạt động như thế nào trong các giao dịch Bitcoin?

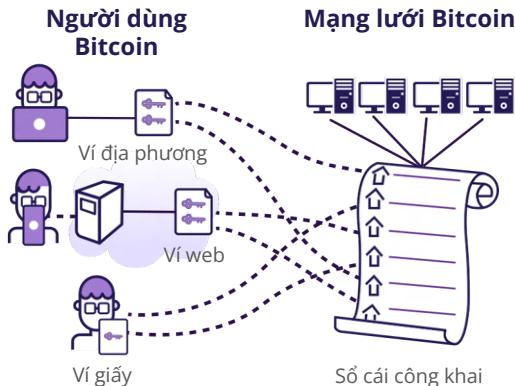
Trong mật mã khóa riêng truyền thống, John và Arel trước tiên phải chia sẻ một khóa bí mật, chẳng hạn như một mật khẩu hoặc bảng mã Pigpen. John sẽ sử dụng khóa này để mã hóa thông điệp trước khi gửi cho Arel. Arel, người cũng biết khóa bí mật, sẽ dùng cùng khóa đó để giải mã và đọc thông điệp.

Tuy nhiên, nếu có ai đó sở hữu khóa này và chặn được thông điệp, họ cũng có thể giải mã và đọc được nội dung.

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

Mật mã khóa công khai, loại được sử dụng trong các giao dịch Bitcoin, đã giải quyết vấn đề này. Với mật mã khóa công khai, John và Arel không cần chia sẻ mật khẩu hoặc phương pháp mã hóa với nhau. Thay vào đó, mỗi người sẽ có hai khóa khác nhau: một **khóa công khai** (có thể chia sẻ với bất kỳ ai) và một **khóa riêng** (cần được giữ bí mật).

Trong trường hợp này, khi John muốn gửi một thông điệp cho Arel, anh ấy có thể sử dụng **khóa công khai** của Arel để mã hóa thông điệp trước khi gửi đi. Khi Arel nhận được thông điệp, chỉ mình anh ấy mới có thể giải mã bằng **khóa riêng** của mình. Người khác, ngay cả khi chặn được thông điệp, cũng sẽ không thể đọc được nội dung. Ngay cơ bị đánh cắp khóa cũng thấp hơn nhiều vì ngay cả John và Arel cũng không cần chia sẻ khóa riêng với nhau.



Vì vậy, lợi thế chính của mật mã khóa công khai so với khóa riêng là nó cho phép giao tiếp an toàn mà không cần người gửi và người nhận phải chia sẻ trước một khóa bí mật (hoặc phương pháp mã hóa khác như bảng mã Pigpen), vốn có thể bị bên thứ ba chặn được.

Trong Bitcoin, mật mã khóa công khai không được dùng để gửi các thông điệp đã mã hóa. Thay vào đó, nó được sử dụng để tạo ra **chữ ký số** độc nhất, giúp các giao dịch bitcoin không thể bị thay đổi. **Chữ ký số** là một cách để chứng minh tính xác thực của một giao dịch bitcoin, tương tự như khi bạn ký tên vào một tài liệu giấy.

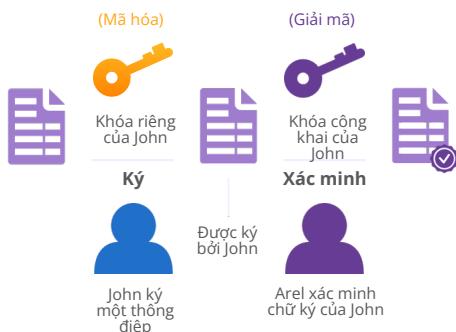
Mật mã khóa công khai (cho mỗi giao dịch giữa hai người dùng):

Mỗi người dùng có hai khóa: một **khóa riêng**, được giữ bí mật, và một **khóa công khai** có thể chia sẻ với người khác.

Khóa riêng đóng vai trò như một hình thức nhận dạng và bằng chứng sở hữu, xác nhận rằng: **"Địa chỉ này thuộc về tôi và tôi có quyền kiểm soát nó."**

Chữ ký số được tạo ra để xác định từng giao dịch một cách duy nhất.

Chữ ký số



- ◆ Giao dịch Bitcoin liên quan đến việc chuyển một lượng bitcoin nhất định trực tiếp đến tài khoản của người khác.
- ◆ Mã hóa được sử dụng để đảm bảo chỉ chủ sở hữu thật sự của bitcoin mới có quyền kiểm soát và gửi tiền cho người khác. Nó giúp bảo vệ tài sản khỏi các hành vi xấu.
- ◆ Để tăng cường bảo mật, mỗi giao dịch bạn gửi trong mạng Bitcoin đều tự động có một **chữ ký số ĐỘC NHẤT**. **Chữ ký số độc nhất** này được bảo vệ bằng công nghệ chống giả mạo, giúp mạng lưới xác minh rằng chính chủ sở hữu bitcoin, chứ không phải ai khác, là người đã gửi giao dịch.

Alice [Tài khoản tiền mặt]

Ghi nợ	Ghi có
	\$100

Bob [Tài khoản tiền mặt]

Ghi nợ	Ghi có
\$100	

Số cái công khai (Biên lai điện tử)

Alice	Bob
\$100	\$100
Ra	Vào
Chữ ký	Chữ ký

Giải thích đơn giản về cách điều này hoạt động trong một giao dịch Bitcoin thực tế:

1 Tạo giao dịch:

Người dùng bắt đầu một giao dịch bitcoin bằng cách nhập các thông tin như địa chỉ của người nhận và số lượng bitcoin muốn gửi.

2 Tạo chữ ký số:

Người gửi tạo một **chữ ký số** độc nhất bằng **khóa riêng** của mình. Đây là một mã duy nhất dùng để xác minh tính xác thực của giao dịch.

3 Phát sóng giao dịch:

Giao dịch đã được ký sẽ được phát tới mạng lưới Bitcoin, thể hiện ý định chuyển quyền sở hữu bitcoin từ người gửi sang người nhận.

4 Xác minh trên mạng lưới:

Các nút trong mạng Bitcoin nhận giao dịch và sử dụng **khóa công khai** của người nhận để giải mã và kiểm tra tính toàn vẹn của giao dịch. Đồng thời, họ cũng dùng **khóa công khai** của người gửi để xác minh **chữ ký số**.

5 Xác nhận trên mạng Bitcoin:

Nếu việc xác minh thành công, giao dịch sẽ được thêm vào sổ cái, đóng vai trò là bản ghi minh bạch và an toàn cho tất cả giao dịch. Khi đã được xác nhận, quyền sở hữu bitcoin sẽ chính thức được chuyển từ người gửi sang người nhận.



Tóm lại, chữ ký số được tạo bằng khóa riêng của người gửi đóng vai trò là bằng chứng mật mã cho tính xác thực và quyền sở hữu, cho phép mạng lưới phi tập trung của Bitcoin xác minh và ghi lại giao dịch vào sổ cái.

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.1.2 Giải thích hàm băm

Đừng quá lo lắng về các thuật ngữ kỹ thuật và những khái niệm toán học phía trước nhé. Chúng tôi hiểu rằng không phải ai cũng “mặn mà” với toán học, nhưng bạn có thể sẽ rất ngạc nhiên khi thấy ngay cả những ý tưởng phức tạp nhất cũng có thể nắm bắt được chỉ với một chút cỗ gắng.

Hàm là gì?

Hàm giống như một chiếc máy nhận vào một số thông tin rồi biến chúng thành một thứ mới. Thông tin bạn đưa vào hàm gọi là **đầu vào**. Thông tin mới mà hàm tạo ra gọi là **đầu ra**. Hàm giúp máy tính thực hiện các công việc và giải quyết các vấn đề.



Hãy tưởng tượng nó như một công thức làm món salad. Công thức (hay hàm) cho bạn biết cần những nguyên liệu gì và cách trộn chúng với nhau để làm ra món salad. Bạn có thể cho vào các nguyên liệu khác nhau, nhưng công thức sẽ luôn tạo ra món salad ở đầu ra. Hàm được sử dụng để giúp công việc trở nên dễ dàng và hiệu quả hơn.

Công thức này chính là một hàm nhận các nguyên liệu làm **đầu vào** và tạo ra món salad trộn làm **đầu ra**.

Trong Bitcoin, các hàm được dùng để thực hiện các giao dịch. Chúng ta đã biết giao dịch bitcoin về cơ bản là việc chuyển giá trị (tiền) từ địa chỉ này sang địa chỉ khác. Để thực hiện giao dịch, một số hàm mật mã được sử dụng để xác thực giao dịch và cập nhật trạng thái sổ cái của Bitcoin.



Các hàm được sử dụng trong một giao dịch bitcoin bao gồm xác minh tính xác thực của các đầu vào giao dịch, kiểm tra xem người gửi có đủ số dư hay không, và cập nhật số dư của các địa chỉ liên quan. Khi một giao dịch được xác minh và thêm vào một khối trong sổ cái, nó sẽ trở thành một phần của hồ sơ vĩnh viễn ghi lại tất cả các giao dịch trên mạng lưới.

Hàm một chiều là gì?

Hàm một chiều sử dụng một tập hợp các hướng dẫn để xử lý thông tin và biến nó thành một thứ mới, giống như công thức làm sinh tố biến các nguyên liệu thành một món đồ uống mới. Nhưng cũng như bạn không thể tách lại sinh tố để lấy nguyên liệu ban đầu, bạn cũng không thể đảo ngược hàm một chiều để lấy lại thông tin gốc.



Mật mã khóa công khai, trong đó khóa công khai là một phần, dựa vào việc sử dụng hàm một chiều, tức là loại hàm khiến việc xác định khóa riêng từ khóa công khai trở nên cực kỳ khó khăn. Về mặt lý thuyết, không hẳn là “không thể” tìm ra khóa riêng từ khóa công khai, nhưng điều đó vô cùng khó và sẽ đòi hỏi một lượng lớn thời gian cùng sức mạnh tính toán.

Việc tìm khóa riêng từ khóa công khai trong Bitcoin giống như cố gắng tìm một cây kim trong một đống cỏ khô rộng bằng cả một sân bóng đá. Cây kim tượng trưng cho khóa riêng, còn đống cỏ khô đại diện cho tất cả các khóa riêng có thể tồn tại. Tương tự như vậy, hàm một chiều được thiết kế để không thể đảo ngược và không thể giải mã theo cách thông thường.



Hàm băm là gì?

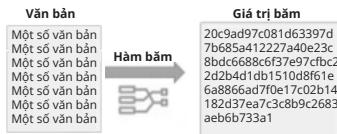
Quá trình băm giống như dấu vân tay của thông tin kỹ thuật số. Đó là quá trình lấy một thông điệp kỹ thuật số và chuyển đổi nó thành một mã có độ dài cố định, đóng vai trò như một định danh duy nhất.



Cũng giống như dấu vân tay có thể nhận diện một người, giá trị băm có thể nhận diện một thông điệp số. Giá trị băm được sử dụng trong nhiều ứng dụng, bao gồm cả các giao dịch Bitcoin.

Cách băm được sử dụng trong các giao dịch Bitcoin

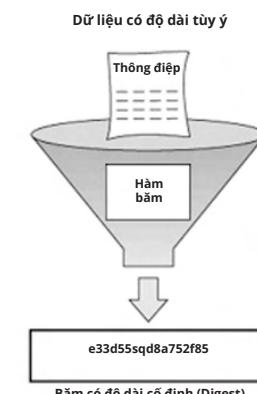
Trong Bitcoin, mỗi giao dịch đều được băm trước khi được thêm vào một khối trong sổ cái. Giá trị băm đóng vai trò như một chữ ký kỹ thuật số, giúp xác minh rằng giao dịch đó hợp lệ và chưa bị can thiệp. Nếu ai đó cố thay đổi dù chỉ một ký tự trong giao dịch, giá trị băm sẽ hoàn toàn khác biệt, báo hiệu cho mọi người biết có sự thay đổi xảy ra.



Vai trò của băm trong việc đảm bảo an ninh

Băm đóng vai trò thiết yếu trong việc bảo vệ an ninh cho mạng lưới Bitcoin. Bằng cách sử dụng giá trị băm để nhận diện các giao dịch, mạng lưới có thể phát hiện bất kỳ nỗ lực thay đổi hoặc thao túng giao dịch nào. Điều này giúp ngăn chặn gian lận và đảm bảo mọi giao dịch đều được ghi lại chính xác trên sổ cái.

Hàm băm là một loại hàm một chiều, nhận một đầu vào (gọi là “thông điệp” hoặc “dữ liệu”) và chuyển đổi nó thành một dạng số gọi là “giá trị băm.” Giá trị băm đầu ra là duy nhất cho từng dữ liệu đầu vào, nên ngay cả một thay đổi nhỏ trong dữ liệu đầu vào cũng sẽ tạo ra một giá trị băm hoàn toàn khác biệt.



Hàm băm giống như một cỗ máy mã hóa bí mật. Nó nhận vào một **thông điệp** và biến nó thành một đoạn mã.



Giới thiệu về khía cạnh kỹ thuật của Bitcoin

Đoạn mã luôn giống nhau nếu thông điệp không thay đổi. Nhưng nếu bạn thay đổi thông điệp dù chỉ một chút, đoạn mã sẽ hoàn toàn khác. Điều này giúp máy tính ghi nhớ và kiểm tra xem thông tin có bị thay đổi hay không.



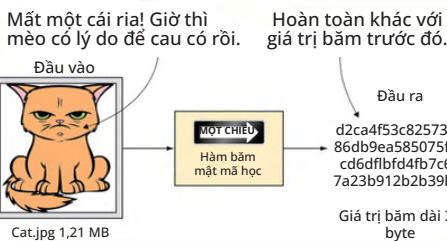
Tạo giá trị băm SHA256 của bất kỳ chuỗi hoặc giá trị đầu vào nào một cách tức thì. Hàm băm được sử dụng như một phương pháp mật chiết.

Hoạt động: Tạo mã băm SHA-256 →



Đầu vào
Cat.jpg 1,21 MB

Đầu ra
dee6a5d375827436
ee4b47a930160457
901dce84ff0fac58
bf79ab0edb479561
Giá trị băm dài 32 byte



Mất một cái ria! Giờ thì mèo có lý do để cau có rồi. Hoàn toàn khác với giá trị băm trước đó.
Đầu vào
Cat.jpg 1,21 MB
Đầu ra
d2ca4f53c8257301
86db9ea585075f96
cd6dfbf4fb7c68
7a23b912b2b39bf6
Giá trị băm dài 32 byte

Đầu ra, hay còn gọi là giá trị băm, luôn có độ dài cố định, bất kể thông tin gốc dài bao nhiêu.

Bitcoin sử dụng một vài loại hàm băm cụ thể, gọi là **SHA-256** và **RIPEMD160**. Một vài ví dụ được đưa ra bên dưới:

💡 Hãy chú ý rằng chỉ một thay đổi nhỏ trong đầu vào thứ hai đã khiến đầu ra hoàn toàn khác so với đầu vào đầu tiên.

💡 Đầu vào thứ ba là một tập tin rất lớn, nhưng đầu ra vẫn có độ dài cố định như hai cái trước.

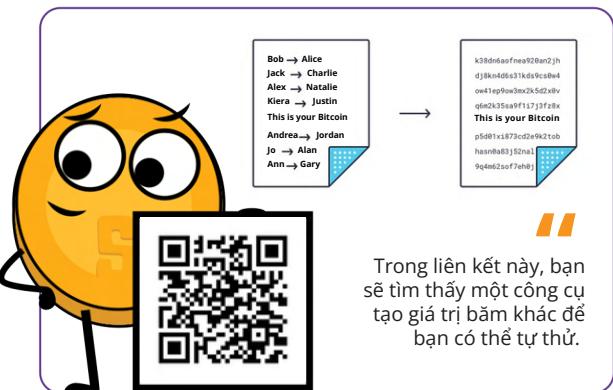
- • • • •
- Giá trị băm SHA256 của chuỗi **xin chào thế giới**
B94d27b9934d3e08a52e52d7da7dabfac484fe37a5380ee9088f7ace2efcde9
- Giá trị băm SHA256 của chuỗi **xin chào thế giới**.
7ddb227315f423250fc673be69c544628dff41752af91c50ae0a9c49faeb87
- Giá trị băm SHA256 của tập tin ISO có thể tải về **Ubuntu 18.10**
7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765
- • • • •

Quá trình băm cũng có thể được hiểu như một bản nhạc ghi lại tinh túy của một tác phẩm âm nhạc. Cũng giống như bản nhạc là một biểu diễn duy nhất của một giai điệu, giá trị băm là một biểu diễn duy nhất của một đoạn dữ liệu. Bằng cách so sánh bản nhạc với màn trình diễn thực tế, nhạc sĩ có thể xác định xem màn trình diễn có chính xác hay không. Tương tự, bằng cách so sánh giá trị băm của dữ liệu nhận được với giá trị băm ban đầu, người ta có thể phát hiện xem dữ liệu có bị thay đổi trong quá trình truyền tải hay không.



Cũng như một sai lệch nhỏ trong màn trình diễn âm nhạc có thể làm cho âm thanh khác đi, ngay cả thay đổi nhỏ nhất trong dữ liệu gốc cũng sẽ tạo ra một giá trị băm khác biệt. Điều này khiến băm trở thành một công cụ mạnh mẽ để đảm bảo tính toàn vẹn và tính xác thực của một giao dịch Bitcoin.

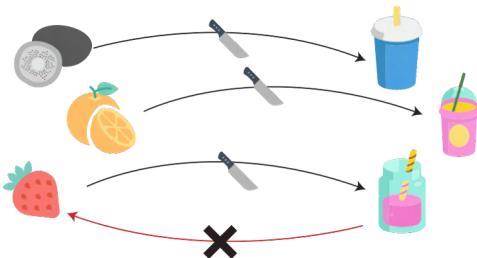
Quá trình mã hóa khóa công khai thông qua băm được sử dụng để nâng cao bảo mật thông tin bằng cách chuyển đổi nó thành định dạng có độ dài cố định và không đọc được. Bitcoin sử dụng các thuật toán SHA-256 và RIPEMD-160 để tạo ra địa chỉ công khai. Kết quả đầu ra này đóng vai trò như một định danh duy nhất cho khóa công khai và giúp đảm bảo tính toàn vẹn cùng an ninh của các giao dịch được lưu trữ trên sổ cái. Bằng cách mã hóa thông tin theo cách này, việc truy cập và thao túng dữ liệu trái phép trở nên khó khăn hơn nhiều.



Quá trình băm

Hàm băm nhận bất kỳ đầu vào nào và tạo ra một đầu ra có độ dài cố định (giá trị băm).

Thành phần **Hàm băm** **Sinh tố**



Tính quyết định.

Cùng một công thức nguyên liệu luôn cho ra cùng một loại sinh tố.

Kháng tiền ản.

Khi đã có ly sinh tố, bạn không thể tách ra được quả dâu tây ban đầu.

Kháng tương quan.

Thay đổi một chút nguyên liệu sẽ tạo ra một ly sinh tố hoàn toàn khác.

Kháng va chạm.

Rất khó tìm được hai công thức nguyên liệu khác nhau mà tạo ra cùng một ly sinh tố giống hệt nhau.

Tốc độ và khả năng kiểm tra.

Cho trái cây vào máy xay. Quá trình nhanh chóng và chắc chắn bạn sẽ có một ly sinh tố.

9.2 Mô hình UTXO

UTXO – Đầu ra giao dịch chưa được chi tiêu

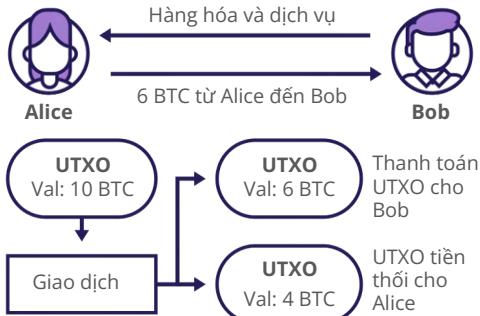


Giới thiệu về khía cạnh kỹ thuật của Bitcoin

UTXO là gì?

Trong Bitcoin, các giao dịch hoạt động giống như việc bạn đập một thỏi vàng lớn thành những mảnh nhỏ hơn để gửi cho người khác và cả cho chính mình.

Bạn có thể nghĩ về UTXO như các kích cỡ và mệnh giá bitcoin khác nhau trong ví của bạn. Khi bạn chi tiêu một UTXO, nó được tạo lại thành một UTXO mới cho người nhận, và bất kỳ phần dư nào sẽ được gửi lại cho bạn trong một UTXO mới khác được gọi là "UTXO tiền thối." Điều này giống như việc dùng một tờ 10 đô để mua hai ly cà phê giá 6 đô. Quán cà phê giữ lại phần 6 đô và đưa lại cho bạn 4 đô tiền thối.



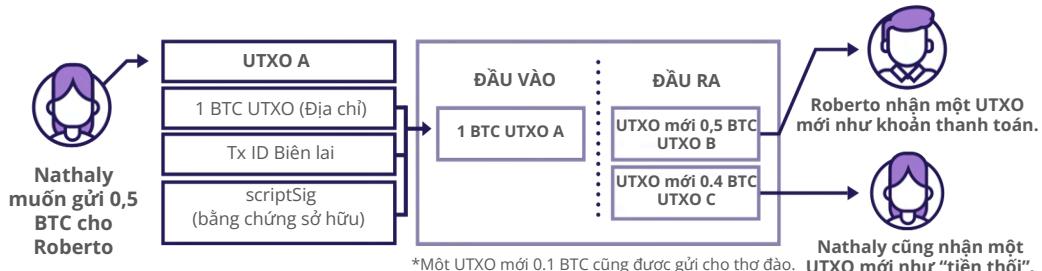
Khi gửi bitcoin, bạn luôn gửi toàn bộ giá trị của một (hoặc nhiều) UTXO trong ví Bitcoin của mình. Chuyện gì xảy ra? Bạn gửi một phần cho người nhận và nhận lại phần còn lại dưới dạng tiền thối vào một địa chỉ Bitcoin mới của bạn. Phần tiền thối bạn nhận lại được gọi là đầu ra giao dịch chưa được chi tiêu, hay UTXO, và nó có thể được sử dụng làm đầu vào cho một giao dịch mới trong tương lai.

Số dư trong ví Bitcoin của bạn là tổng của tất cả các UTXO khác nhau mà bạn sở hữu. Vì vậy, tổng các UTXO của bạn chính là tổng số bitcoin bạn đang nắm giữ.



Điều quan trọng cần lưu ý là bạn không nên để người khác biết về các UTXO của mình, vì khi ai đó biết được chúng, họ có thể theo dõi các giao dịch bitcoin của bạn trên mạng lưới và cuối cùng sẽ biết bạn sở hữu bao nhiêu tiền.

Tóm lại, mỗi khi bạn thực hiện một giao dịch, bạn sử dụng một hoặc nhiều UTXO hiện có để chi tiêu bitcoin, và các UTXO mới sẽ được tạo ra (bao gồm cả cho bạn nếu bạn là người nhận).



Khi một giao dịch được thực hiện, số lượng bitcoin được gửi sẽ được chia thành nhiều đầu ra, mỗi đầu ra gần với một địa chỉ Bitcoin mới (một UTXO mới).

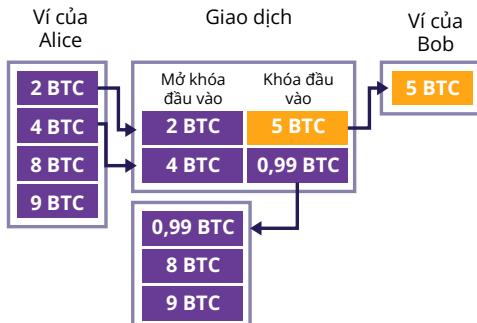
Chương #9

Khi gửi bitcoin cho ai đó, bạn sẽ sử dụng một hoặc nhiều UTXO làm nguồn tiền (đầu vào). Các UTXO này sẽ được kết hợp lại nếu cần thiết để tạo ra các đầu ra mới thuộc về cả người nhận giao dịch và chính bạn. Những đầu ra mới này, hay UTXO, sẽ trở thành tài sản của người nhận và của bạn. Sau đó, các UTXO này có thể được sử dụng làm nguồn tiền trong các giao dịch tiếp theo. Chuỗi các UTXO như vậy tạo ra một lịch sử minh bạch và có thể truy vết của tất cả các giao dịch bitcoin trên sổ cái của Bitcoin, bắt đầu từ khối đầu tiên (ngày 3 tháng 1 năm 2009).

Một ví dụ để minh họa cách hoạt động này: nếu bạn muốn gửi 2 bitcoin nhưng chỉ có một UTXO trị giá 5 bitcoin, thì phần chênh lệch 3 bitcoin sẽ được gửi lại cho bạn dưới dạng "tiền thối". Khoản tiền thối này là một UTXO mới dành cho bạn, và bạn có thể sử dụng UTXO đó trong các giao dịch tương lai.

Một ví dụ khác:

- 1 Alice muốn gửi cho Bob 5 bitcoin.
- 2 Cô ấy kết hợp 6 bitcoin từ hai UTXO của mình.
- 3 Từ các UTXO này, cô gửi 5 bitcoin cho Bob, nhận lại 0,99 bitcoin tiền thối và trả 0,01 bitcoin phí giao dịch.
- 4 Sau khi được xác nhận, giao dịch sẽ được thêm vào sổ cái của Bitcoin, cập nhật tất cả các nút đang lưu trữ bản sao của sổ cái.



Nếu Alice cố gắng sử dụng một đầu ra đã được tiêu (đã sử dụng) để thực hiện một giao dịch khác, giao dịch đó sẽ tự động bị các nút từ chối. Điều này là do các nút đều lưu trữ một bản sao của sổ cái Bitcoin (bao gồm tất cả các giao dịch), nên họ có thể dễ dàng kiểm tra số dư UTXO của Alice và xác minh rằng giao dịch không hợp lệ.



Dưới đây là ảnh chụp màn hình thực tế của một giao dịch thật, trong đó chỉ có một đầu vào. Tuy nhiên, trong những trường hợp khác, số dư ban đầu có thể là tổng của nhiều UTXO (nhiều đầu vào). Bạn có thể rút ra những nhận xét gì khi quan sát hai giao dịch bên dưới? Liệu tổng đầu vào có khớp với tổng đầu ra không? Bạn có thể mô tả chi tiết giao dịch đó không? Có mối liên hệ nào giữa hai ảnh chụp màn hình không? Và giao dịch nào xảy ra trước?

total value
฿ 24.34898570

1 đầu vào 2 đầu ra + phí

total value
฿ 24.34901060

3 đầu vào 2 đầu ra + phí

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.3 Nhìn kỹ hơn vào các nút Bitcoin và thợ đào

Trong phần này, chúng ta sẽ xem xét kỹ hơn hai thành phần rất quan trọng (và những người tham gia) trong mạng Bitcoin đã được giới thiệu ở Chương 6. Chúng ta sẽ tìm hiểu về:



Các nút Bitcoin:

1

Là những người gác cổng xác nhận, nhiệm vụ chính là giữ một bản sao của sổ cái Bitcoin, đảm bảo tất cả các giao dịch đều hợp lệ và mọi người đều tuân theo cùng một bộ quy tắc.

Bằng cách phân phối công việc này cho nhiều người trên khắp thế giới, Bitcoin trở nên mạnh mẽ trước các vấn đề tiềm ẩn. Các nút này giúp giữ cho hệ thống đáng tin cậy và trung thành với ý tưởng phi tập trung, nơi không một cá nhân hay nhóm nào có quá nhiều quyền lực.



Thợ đào Bitcoin:

2

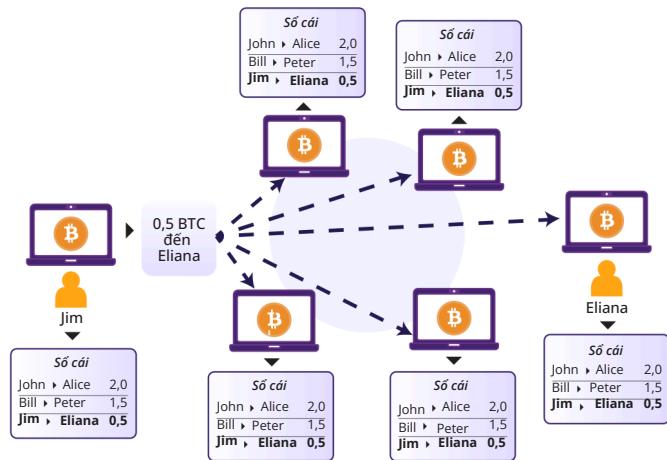
Là những kiến trúc sư của bảo mật, sử dụng máy tính mạnh mẽ và điện năng để kiểm tra và xác nhận các giao dịch, đảm bảo mọi thứ đều an toàn. Công việc này giúp làm cho sổ cái, hay blockchain, trở nên khó bị tấn công bởi những kẻ xấu muốn phá hoại.

Các nút và thợ đào Bitcoin cùng nhau hợp tác như một đội để duy trì một hệ thống phi tập trung, an toàn và vững mạnh — một cách thức mới để quản lý tiền mà mọi người trên khắp thế giới có thể tin tưởng. Hãy cùng tìm hiểu chi tiết hơn về các vai trò này để hiểu cách chúng góp phần vào hệ thống Bitcoin đầy sáng tạo.

9.3.1 Nút Bitcoin là gì và cách làm thế nào để thiết lập một nút?

Một nút Bitcoin có thể nghe có vẻ kỹ thuật, nhưng thực ra nó chỉ là một phần mềm chạy bản sao của sổ cái Bitcoin. Khi bạn vận hành nút Bitcoin của riêng mình, bạn có tiếng nói trong việc định hình các quy tắc của mạng Bitcoin.

Hãy tưởng tượng như thế này: nếu một nhóm người cố gắng thay đổi cách Bitcoin hoạt động, chẳng hạn như thay đổi tổng cung bitcoin, bạn có quyền quyết định. Bạn có thể chọn không cập nhật nút của mình theo hệ thống mới, giống như việc bỏ phiếu để giữ vững các quy tắc mà bạn ủng hộ trong mạng lưới.



Hãy tưởng tượng một nút Bitcoin như một cảnh sát giao thông kỹ thuật số với một số nhiệm vụ quan trọng:

Người gác cống xác nhận:

1 Một nút Bitcoin lưu giữ một bản sao kỹ thuật số của blockchain , giống như một số cái dùng chung ghi lại tất cả các giao dịch Bitcoin. Nhiều nút trên khắp thế giới đều giữ bản ghi giống hệt này.

Trung tâm giao tiếp:

2 Các nút kết nối với nhau, tạo thành một mạng lưới giao tiếp rộng lớn. Chúng chia sẻ thông tin, đặc biệt là các giao dịch đang chờ được thêm vào blockchain , và được lưu trữ trong một “phòng chờ” kỹ thuật số gọi là mempool.

Người kiểm tra chất lượng:

3 Mỗi lần blockchain được cập nhật đều trải qua quá trình kiểm tra nghiêm ngặt. Các nút đảm bảo rằng các giao dịch hợp lệ và từ chối bất kỳ giao dịch nào không tuân theo các quy tắc của mạng Bitcoin.

Người cung cấp thông tin blockchain:

4 Các phần mềm khác, như ví điện tử, có thể yêu cầu thông tin từ các nút về blockchain , chẳng hạn như số dư Bitcoin. Các nút đóng vai trò như trung tâm cung cấp thông tin.

Người chào đón nút mới:

5 Khi một nút mới muốn tham gia mạng, các nút hiện có sẽ cung cấp một bản sao blockchain . Nút mới sẽ tự mình kiểm tra tính hợp lệ của từng giao dịch, nhấn mạnh tính phi tập trung và không cần tin cậy của hệ thống.

Hoạt động:
Xem video về
các nút Bitcoin



Một trong những cách để vận hành nút riêng của bạn là tải phần mềm Bitcoin Core và dành thời gian để nó tải xuống toàn bộ blockchain . Khi đã sẵn sàng, bạn có thể để nút chạy liên tục. Cứ khoảng 10 phút, các khối mới chứa giao dịch sẽ đến. Nút của bạn sẽ kiểm tra tính hợp lệ của các khối này và thêm chúng vào bản sao blockchain cục bộ của bạn.

Tài nguyên:
Phần mềm
Bitcoin Core



Việc vận hành một nút mang lại quyền kiểm soát và tính độc lập. Bạn không cần phụ thuộc vào người khác. Nó giống như cảnh sát giao thông riêng của bạn vậy. Khác với ví Bitcoin, vốn không có bản sao blockchain , một nút giúp bạn tự chủ hoàn toàn. Thay vì phải tin vào người khác về số dư Bitcoin của bạn hay tình trạng của mạng Bitcoin, ví của bạn sẽ giao tiếp trực tiếp với nút cá nhân, giúp trải nghiệm số hóa của bạn an toàn và đáng tin cậy hơn.

9.3.2. Thợ đào Bitcoin là gì và quá trình đào hoạt động như thế nào?

Mục đích của việc khai thác không phải là tạo ra bitcoin mới; đó chỉ là phần thưởng khuyến khích. Việc khai thác chính là cơ chế để bảo mật của Bitcoin được phân quyền.

Andreas M. Antonopoulos

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

Các **thợ đào** thu thập các giao dịch chưa được xác nhận, tạo thành một khối, và tiêu tốn năng lượng để tìm một khóa giá trị nhằm **thêm và bảo vệ vị trí của khối đó trong blockchain**.



Các thợ đào đang trong cuộc đua để thêm khối tiếp theo vào blockchain. Phần thưởng được săn đón là một "giá trị băm khối hợp lệ" được giấu kín giữa hàng tỷ giá trị khác, và chỉ có một khóa đặc biệt do mạng lưới chỉ định mới có thể mở được.

Hãy tưởng tượng một đồng rơm khổng lồ chứa hàng triệu chiếc chìa khóa, mỗi chiếc tương trưng cho một giá trị băm khối duy nhất. Mạng lưới đã chọn ra một chiếc chìa khóa đặc biệt để mở phần thưởng giá trị. Các thợ đào lục lọi trong đồng rơm, thử từng chiếc chìa khóa trên ổ khóa, nhưng chỉ có một thợ đào may mắn tìm ra chiếc chìa khóa hoàn hảo.

Khi một thợ đào tìm được giá trị băm khôi chính xác, họ sẽ chia sẻ với mạng lưới cùng với khối giao dịch mới mà họ tạo ra. Các thợ đào khác sẽ xác minh giải pháp để đảm bảo nó chính xác. Nếu mọi thứ hợp lệ, khối sẽ được thêm vào blockchain, tạo nên một sổ cái công khai và an toàn.

Các thợ đào nhận được phần thưởng cho nỗ lực của mình theo hai cách:

1

Phần thưởng khôi

2

Phí giao dịch

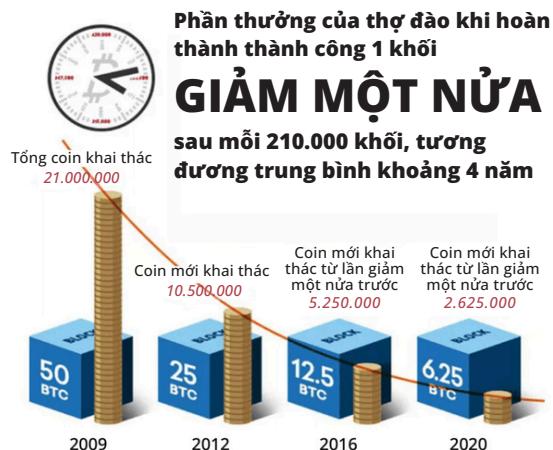
Phần thưởng khôi là số bitcoin mới được phát hành vào lưu thông mỗi khi một khôi được thêm vào blockchain. Phí giao dịch là khoản thanh toán nhỏ bằng bitcoin mà người dùng trả để giao dịch của họ được xử lý nhanh hơn và được thợ đào ưu tiên. Các thợ đào có thể chọn giao dịch nào để đưa vào khôi mà họ khai thác, thường ưu tiên những giao dịch có phí cao hơn.

Bitcoin giảm một nửa

Một lần giảm một nửa trong Bitcoin là yếu tố cốt lõi giúp duy trì tính khan hiếm và giá trị của nó theo thời gian. Như bạn đã biết, tổng nguồn cung của Bitcoin được giới hạn ở mức 21.000.000 bitcoin. Tuy nhiên, số lượng này không được phát hành hết ngay từ ngày Bitcoin ra đời. Thay vào đó, nguồn cung được đưa vào hệ thống một cách tuần tự theo từng giai đoạn.

Satoshi Nakamoto đã thiết kế một hệ thống phần thưởng khôi đầy thông minh để phân phối bitcoin mới mà không cần đến bất kỳ cơ quan trung ương nào. Vào những ngày đầu của Bitcoin, các thợ đào nhận được phần thưởng lên đến 50 bitcoin cho mỗi khôi khai thác thành công, tạo động lực lớn để họ đầu tư vào thiết bị mạnh và tiêu tốn điện năng cho hoạt động đào.

Để giữ cho mạng lưới ổn định và kiểm soát nguồn cung bitcoin mới, phần thưởng khôi sẽ được giảm một nửa sau khoảng mỗi 210.000 khôi. Sự kiện này, gọi là "giảm một nửa", làm giảm số lượng bitcoin mới được đưa vào lưu thông và tiếp tục tạo động lực cho thợ đào bảo vệ mạng lưới cũng như duy trì tính phi tập trung. Trong quá khứ, các lần giảm một nửa thường dẫn đến những đợt tăng giá đáng kể trên thị trường Bitcoin, do nguồn cung bitcoin mới bị hạn chế khi đưa vào lưu thông.

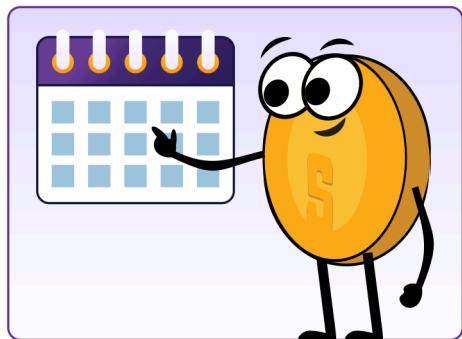


Nguồn cung lưu hành đề cập đến tổng lượng tiền tệ đang có mặt trên thị trường. Đối với Bitcoin, nguồn cung lưu hành là số lượng coin đã được khai thác và đang lưu thông tại một thời điểm nhất định, không bao gồm những coin đã bị mất vĩnh viễn.



Trong mỗi lần giảm một nửa, phần thưởng bitcoin mà thợ đào nhận được sẽ giảm, làm chậm tốc độ phát hành coin mới. Do đó, độ khó khai thác của Bitcoin sẽ tăng lên để duy trì thời gian tạo khối khoảng 10 phút, đảm bảo rằng các khối mới được thêm vào blockchain một cách ổn định. Việc giảm phần thưởng không nhất thiết khiến thợ đào kiếm được ít lợi nhuận hơn, vì họ còn có thể nhận phí giao dịch từ việc xác minh và thêm giao dịch vào blockchain. Điều này giúp bù đắp phần nào cho phần thưởng bị giảm.

Các sự kiện giảm một nửa được lập trình sẵn trong giao thức Bitcoin, giúp cho lịch phát hành bitcoin trở nên minh bạch và có thể dự đoán trước.

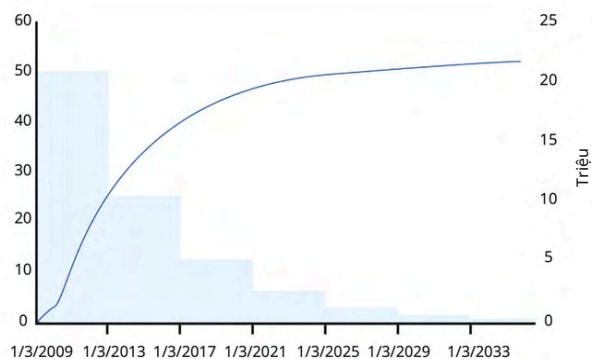


Lịch phát hành nguồn cung của Bitcoin là kế hoạch cố định và công khai về việc đưa bitcoin mới vào lưu thông, được thiết kế để duy trì tính khan hiếm của Bitcoin theo thời gian.



Bảng sau trình bày chi tiết về các sự kiện giảm một nửa sắp tới của Bitcoin, bao gồm ngày dự kiến của lần giảm một nửa tiếp theo, số khối tại thời điểm giảm một nửa, phần thưởng khối (cho mỗi khối được khai thác) trong sự kiện đó, và tỷ lệ phần trăm tổng nguồn cung sẽ được khai thác.

Lịch phát hành nguồn cung Bitcoin



Sự kiện	Ngày dự kiến	Số khối	Phần thưởng khối	Phần trăm đã khai thác
Lần giảm một nửa thứ tư	2024	840.000	3,125	96,875%
Lần giảm một nửa thứ năm	2028	1.050.000	1,5625	98,4375%
Lần giảm một nửa thứ sáu	2032	1.260.000	0,78125	99,21875%

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

Khi ngày càng có nhiều bitcoin được khai thác, nguồn cung lưu hành và tỷ lệ so với tổng nguồn cung sẽ tiếp tục tăng cho đến khi đạt giới hạn tối đa là 21.000.000 bitcoin. Nguồn cung giảm dần kết hợp với nhu cầu giá tăng có thể đẩy giá bitcoin lên (so với đô la Mỹ). Điều này mang lại lợi ích cho những người tham gia sớm và cũng tạo động lực cho thợ đào tiếp tục bảo vệ mạng lưới, đóng góp sức mạnh tính toán và tài nguyên của họ.

Bitcoin: Phần trăm đã khai thác trên tổng 21 triệu



Băm khối (Block Hash) hợp lệ trong Bitcoin là gì?

Trong Bitcoin, một băm khối hợp lệ giống như một mã đặc biệt mà các thợ đào cố gắng tìm ra. Đây là một con số duy nhất giúp theo dõi từng khối trong blockchain, nơi lưu trữ thông tin về các giao dịch. Các khối này kết nối thành chuỗi, từ khối đầu tiên (Genesis block - khối khởi nguyên) đến khối mới nhất, tạo thành bản ghi công khai của tất cả các giao dịch. Băm khối rất quan trọng vì nó liên kết mỗi khối với khối liền trước, giúp bất kỳ ai cũng có thể kiểm tra lịch sử giao dịch. Nó giống như dấu vân tay của mỗi khối, đảm bảo rằng thông tin là chính xác và an toàn. Băm khối đóng vai trò xác nhận rằng dữ liệu trong khối chưa bị thay đổi.



9ebtsznmf7l4b876c5i 7vo3bbv6kq4gem4ywzpuz



Các khối được "liên kết" với nhau bằng cách thiết lập một mối quan hệ cụ thể giữa các khối. Cụ thể, mỗi khối phải chứa một "dấu vân tay", tức là giá trị băm của dữ liệu từ khối trước đó. Hàm băm có thể rút gọn một thông điệp bất kỳ (chẳng hạn như thông tin trong khối) thành một kích thước cố định (ví dụ: 160 bit), tạo ra một dấu vân tay duy nhất cho thông điệp đó.



Satoshi Nakamoto, người tạo ra Bitcoin, đã khai thác khối đầu tiên với tổng cộng 50 bitcoin.



Cuộc đua để khai thác một khối

Các thợ đào tham gia vào một cuộc cạnh tranh để tìm ra giá trị băm của khối sao cho phù hợp với mục tiêu (một con số đặc biệt) do mạng lưới đặt ra. Thợ đào đầu tiên tìm ra đúng giá trị băm sẽ có quyền thêm khối đó vào blockchain và gán cho nó mã định danh tương ứng. Giải pháp này đóng vai trò xác thực tính hợp lệ của khối.

Quá trình đào có thể được ví như một cuộc đua, nơi mục tiêu là về đích càng nhanh càng tốt. Độ khó để tìm ra giá trị băm của khối được điều chỉnh định kỳ, nhằm đảm bảo rằng mỗi khối vẫn được khai thác trong khoảng 10 phút (khi số lượng thợ đào tăng hoặc giảm). Cơ chế này được gọi là "điều chỉnh độ khó."



Giả sử mạng lưới Bitcoin đặt ra mục tiêu là 1.000. Các thợ đào phải sử dụng sức mạnh tính toán và năng lượng để tìm ra một giá trị băm của khối (một con số cụ thể) nhỏ hơn 1.000. Thợ đào đầu tiên tìm được giá trị băm nhỏ hơn 1.000 sẽ được quyền thêm khối mới vào blockchain và nhận phần thưởng bằng bitcoin.

 Độ khó trong việc đào Bitcoin là thước đo cho mức độ khó khi tìm một giá trị băm hợp lệ đáp ứng mục tiêu do mạng lưới đặt ra. Độ khó được điều chỉnh sau mỗi 2.016 khối, tức khoảng hai tuần một lần, nhằm đảm bảo rằng các khối được thêm vào blockchain với tốc độ ổn định. Độ khó được biểu thị bằng một con số; con số càng cao thì việc tìm ra giá trị băm hợp lệ càng khó.

Ví dụ, xem xét hai giá trị băm khác nhau:

 **Giá trị băm 1:** 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Mức độ khó: 1

 **Giá trị băm 2:** 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK

Mức độ khó: 2

Trong ví dụ này, giá trị băm 2 có mức độ khó cao hơn giá trị băm 1 vì nó dài hơn và có nhiều số 0 ở đầu hơn. Các thợ đào sẽ khó tìm được giá trị băm 2 hơn vì máy tính của họ phải làm nhiều việc hơn.

 Bằng cách tìm ra một giá trị băm hợp lệ của khối, thợ đào chứng minh họ đã thực hiện công việc cần thiết để thêm khối mới vào blockchain và được thưởng bằng bitcoin cùng với phí giao dịch cho nỗ lực của mình. Bằng chứng công việc là phương pháp mà mạng lưới Bitcoin sử dụng để xác thực giao dịch và thêm các khối mới vào blockchain.

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

PoW giữ cho Bitcoin an toàn bằng cách khiến cho bất kỳ ai có ý định xấu cũng khó kiểm soát mạng lưới.

Tóm lại, nhiệm vụ của thợ đào bao gồm:

1

Gom giao dịch thành các khối:

Trong khi các nút xác minh các giao dịch mới đang chờ trong "Mempool," thợ đào chọn một số giao dịch để đưa vào khối ứng viên của họ.

2

Bằng chứng công việc:

Các thợ đào đua để tìm giá trị băm hợp lệ.

3

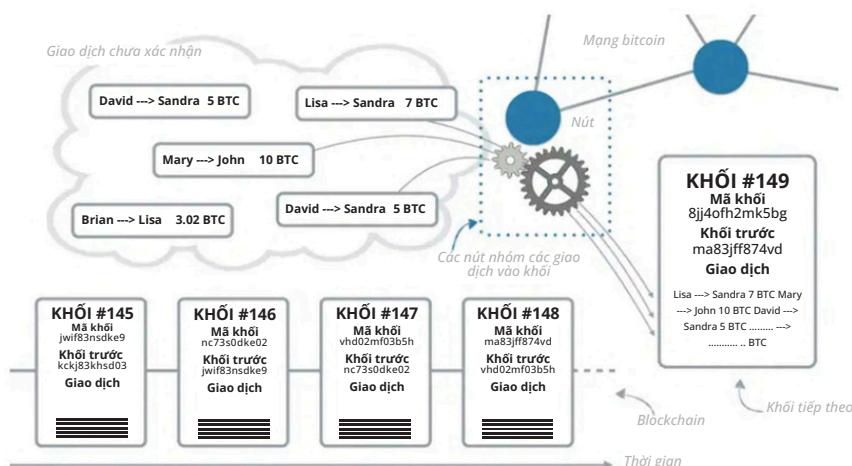
Phát tán các khối hợp lệ:

Sau khi tìm được giá trị băm hợp lệ, họ truyền khối mới đến mạng lưới.

4

Nhận phần thưởng:

Cuối cùng, họ nhận bitcoin mới tạo và phí giao dịch cho việc thêm khối thành công vào blockchain.



Nhiều thợ đào có thể cùng lúc làm việc để tạo các khối mới. Thợ đào đầu tiên tìm ra hàm băm của khối đáp ứng mục tiêu do mạng lưới đặt ra sẽ thông báo kết quả cho mạng. Các thợ đào khác sau đó sẽ kiểm tra các giao dịch trong khối ứng viên của thợ đào đó để đảm bảo rằng chúng hợp lệ. Nếu các giao dịch thực sự hợp lệ, khối đó sẽ được thêm vào blockchain. Các khối được tạo cùng thời điểm bởi những thợ đào khác sẽ không được thêm vào và sẽ bị loại bỏ. Quy trình này giúp duy trì sự đồng thuận trong mạng lưới và ngăn chặn việc chi tiêu gấp đôi.

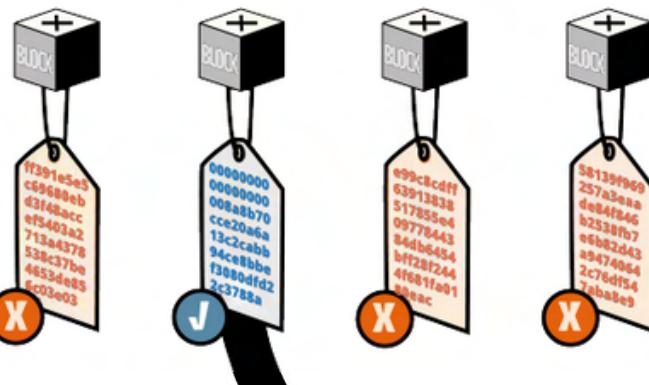
Khối ứng viên là một tập hợp các giao dịch đang được xem xét để thêm vào blockchain, nhưng vẫn chưa được thêm vào.



THỢ ĐÀO –
Là các node làm nhiệm vụ duy trì và cập nhật sổ cái – họ thu thập tất cả dữ liệu giao dịch mới nhất.



Sau đó, họ gom chúng lại thành một **KHỐI** để thêm vào chuỗi.



Tiếp theo, họ tính toán **GIÁ TRỊ BẤM** cho khối đó: chạy toàn bộ dữ liệu qua một thuật toán để tạo ra một chuỗi ký tự duy nhất. Rồi lại làm lại. Và làm lại lần nữa. Họ đang tìm một giá trị băm hợp lệ – một chuỗi bắt đầu bằng nhiều số 0. Người thợ đào đầu tiên tìm được sẽ nhận phần thưởng là bitcoin mới tạo, và khối của họ được thêm vào chuỗi.

Giá trị băm này đảm bảo không ai có thể can thiệp vào sổ cái. Chỉ cần thay đổi một chữ số hoặc ký tự bất kỳ ở bất kỳ đâu trong chuỗi cũng sẽ khiến giá trị băm của tất cả các khối sau đó trở nên **khác biệt đến mức không thể nhận ra**. Khi đó, các node khác sẽ từ chối sổ cái đã bị chỉnh sửa.



9.4 Mempool là gì?

"Mempool" hay bộ nhớ đệm là một dạng phòng chờ dành cho các giao dịch trong mạng Bitcoin. Khi bạn thực hiện một giao dịch, nó sẽ được phát đi và lưu trữ trước tiên trong Mempool trước khi được xác minh, lựa chọn và thêm vào blockchain.

Hãy tưởng tượng bạn đang xếp hàng chờ bàn trong một nhà hàng. Tên bạn được thêm vào danh sách người chờ. Khi có bàn trống, nhân viên sẽ gọi tên bạn và đưa bạn vào ngồi. Tương tự, một giao dịch Bitcoin sẽ được thêm vào Mempool khi được tạo ra, và chỉ được xác nhận và thêm vào blockchain khi một thợ đào đưa nó vào trong một khối.

Giới thiệu về khía cạnh kỹ thuật của Bitcoin

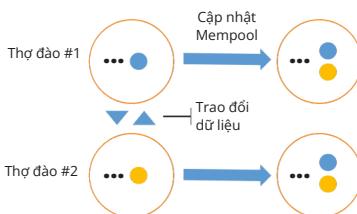
Mempool là nơi các giao dịch chờ được xác nhận và thêm vào khối.

-  tx hsh 6053b699...
phí giao dịch: 3 sat/vB
-  tx hsh bb3b8clfc...
phí giao dịch: 1 sat/vB
-  tx hsh d7c2532a9...
phí giao dịch: 15 sat/vB
-  tx hsh 0ecdcd9c6...
phí giao dịch: 2 sat/vB

Khi một node lần đầu nhận giao dịch từ một node khác, nó phải xác minh giao dịch đó hợp lệ. Không ai muốn các giao dịch sai sót hay gian lận.



Đồng bộ mempool cho phép các node chia sẻ giao dịch của mình với các node khác bằng cách gửi một tin nhắn chứa danh sách các giao dịch đã được **xác minh** trong mempool.



Giao dịch được xác minh và thêm vào Mempool như thế nào?

Khi các giao dịch mới được phát sóng trên mạng Bitcoin, các node sẽ kiểm tra để đảm bảo giao dịch hợp lệ và số tiền chưa bị chi tiêu trước đó. Sau khi giao dịch được xác minh, các node sẽ thêm chúng vào Mempool của mình. Các node tiếp tục chia sẻ giao dịch với các node khác để kiểm tra chéo. Cuối cùng, nếu đa số node đồng ý, các giao dịch sẽ được cung cấp cho thợ đào lựa chọn và thêm vào khối. Tuy nhiên, vẫn có một số lý do khiến giao dịch có thể không được xác nhận sau 72 giờ:

Mục đích chính của **mempool** là:

1

Trung chuyển các giao dịch chưa được xác nhận.



2

Cung cấp giao dịch cho thợ đào khai thác.



Chấp nhận vào Mempool (ATMP) bao gồm việc kiểm tra các yếu tố như:

- Tôi đã có giao dịch này chưa?
- Có xung đột với giao dịch khác trong mempool không?
- Số bitcoin vào có đủ để chi trả cho số bitcoin ra không?
- Chữ ký có chứng minh các đầu ra trước đó có thể chi tiêu được không?
- Phí giao dịch có đủ không?

1**Phí giao dịch thấp:**

Các giao dịch có phí thấp có thể không được xử lý nhanh vì thợ đào thường ưu tiên các giao dịch có phí cao hơn để đưa vào block.

2**Tắc nghẽn mạng:**

Nếu mạng bị tắc nghẽn, việc xác nhận giao dịch có thể bị trì hoãn, ngay cả khi phí giao dịch cao.

3**Cố gắng chi tiêu kép:**

Nếu một tác nhân độc hại cố gắng thực hiện chi tiêu kép, giao dịch của họ có thể bị mạng lưới từ chối.

4**Dữ liệu sai hoặc không đầy đủ:**

Giao dịch chứa dữ liệu sai hoặc không đầy đủ có thể bị từ chối.

5**Giao dịch bị lỗi cấu trúc:**

Giao dịch bị lỗi định dạng cũng có thể bị từ chối.

Để tránh giao dịch bị từ chối, bạn nên đặt mức phí đủ cao để giao dịch được xử lý kịp thời và kiểm tra kỹ tất cả dữ liệu trong giao dịch trước khi gửi.

Hoạt động: Mempool**1**

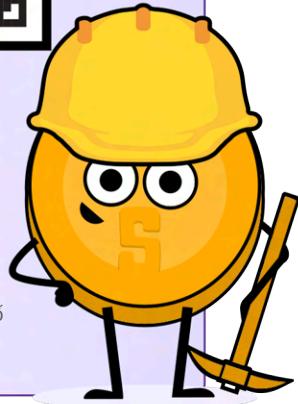
Truy cập trang web:

<https://mempool.space/vi/>

2

Xem xét các yếu tố khác nhau hiển thị trên trang, bao gồm các block mới nhất, các giao dịch đã được xác nhận, số lượng giao dịch, dung lượng bộ nhớ sử dụng và giá trị xấp xỉ của toàn bộ block. Trả lời các câu hỏi sau:

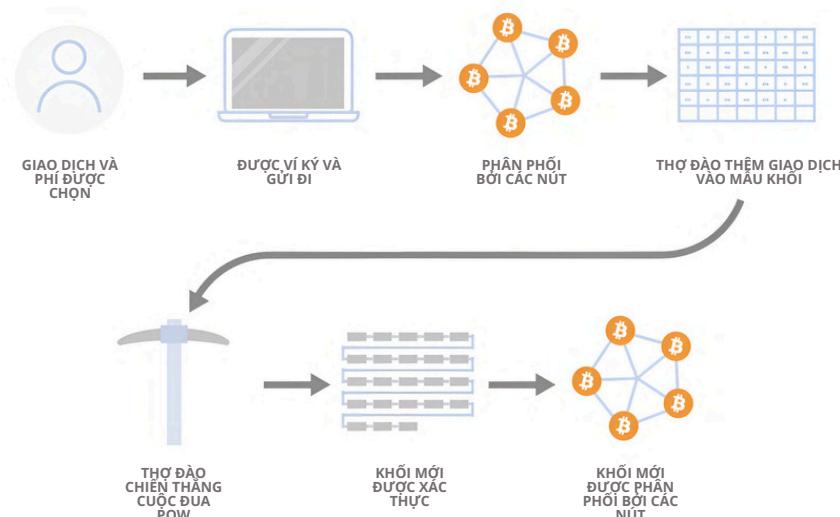
- 👉 Block được khai thác cuối cùng là gì?
- 👉 Có bao nhiêu giao dịch được bao gồm trong block đó?
- 👉 Tổng giá trị giao dịch bằng bitcoin là bao nhiêu?
- 👉 Kích thước block tính theo megabyte là bao nhiêu?
- 👉Nonce của block bắt đầu với bao nhiêu số 0?
- 👉Thợ đào đã kiếm được bao nhiêu bitcoin tổng cộng?
- 👉Tổng giá trị phí thợ đào nhận được khi thêm các giao dịch vào mạng là bao nhiêu?
- 👉 Chọn một trong các giao dịch có giá trị cao nhất trong block. Số lượng địa chỉ Bitcoin mà số tiền đó được phân phối đến là bao nhiêu?



Giới thiệu về khía cạnh kỹ thuật của Bitcoin

9.5 Quy trình hoạt động của một giao dịch Bitcoin từ đầu đến cuối

- 1 Adam muốn gửi bitcoin cho Gerardo. Anh ấy chọn một trong các UTXO của mình, tạo một giao dịch và thêm vào tất cả thông tin cần thiết, bao gồm số lượng bitcoin muốn gửi, địa chỉ nhận của Gerardo và một mức phí giao dịch cao hơn trung bình.
- 2 Sau khi kiểm tra lần cuối để đảm bảo mọi thông tin đều chính xác, Adam sử dụng khóa riêng của mình để ký giao dịch.
- 3 Adam phát sóng giao dịch lên mạng lưới Bitcoin.



Nguồn: Stevenot, Ted, "What is a bitcoin node and how does one work?". Unchained Capital, 17 tháng 1 năm 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

- 4 Các nút trong mạng nhận giao dịch và xác minh tính hợp lệ của nó theo các quy tắc đồng thuận (ví dụ như kiểm tra chữ ký của Adam có hợp lệ không và liệu anh ấy có đủ tiền để thực hiện giao dịch hay không).
- 5 Giao dịch được đánh dấu là hợp lệ và các nút lan truyền nó đến những nút khác trong mạng, đồng thời thêm vào Mempool.
- 6 Vì Adam đã chọn một mức phí giao dịch đủ cao, hầu hết các thợ đào đều đưa giao dịch của anh vào khối của họ.

7

Bằng chứng công việc (Proof-of-Work): Các thợ đào cạnh tranh với nhau và cố gắng khai thác khối của mình bằng cách tìm ra mã băm khối hợp lệ. Một trong số họ tìm được mã băm và phát sóng khối của mình lên mạng.

8

Các nút nhận được khối mới được khai thác và tiến hành xác minh tính hợp lệ của nó. Quá trình này bao gồm việc kiểm tra tất cả các giao dịch trong khối và đảm bảo yêu cầu bằng chứng công việc đã được đáp ứng.

9

Phần lớn các nút đồng ý rằng khối là hợp lệ và thêm nó vào blockchain. Gerardo nhận được số bitcoin đã được xác nhận tại địa chỉ nhận của mình.

10

Khi các khối tiếp theo được thêm vào blockchain trong khoảng một giờ sau đó, số lượng xác nhận của giao dịch cũng tăng lên. Khi số lần xác nhận tăng, Gerardo cảm thấy yên tâm hơn về tính thành công và không thể bị đảo ngược của giao dịch.



Tóm lại, người gửi ký giao dịch bằng khóa riêng của mình, các nút xác minh các UTXO của giao dịch, và các thợ đào thêm giao dịch đã được xác minh vào blockchain. Người nhận sau đó có thể truy cập số bitcoin bằng khóa riêng của họ. Khi một khối được khai thác, tất cả các giao dịch trong khối đó được xem là đã được xác nhận và các UTXO được dùng làm đầu vào cho những giao dịch này được coi là đã sử dụng và sẽ không được dùng lại nữa.

Kết thúc chương này, bạn đã nắm được những khái niệm nền tảng về cách Bitcoin vận hành. Chúng ta đã cùng tìm hiểu từ những kiến thức cơ bản về tiền đến các khía cạnh kỹ thuật của công nghệ Bitcoin. Giờ đây, hãy cùng kết nối mọi thứ lại trong chương tiếp theo. Chương 10 đang chờ đón bạn, nơi chúng ta sẽ khám phá câu hỏi quan trọng: "Tại sao Bitcoin?"

Chương #10

Tại sao Bitcoin?

10.0 Giới thiệu

Hoạt động: Tương lai của Bitcoin có thể trông như thế nào?

10.1 Tiền kỹ thuật số của ngân hàng trung ương (CBDC) là gì và ai kiểm soát chúng?

10.2 Triết lý của Bitcoin

Hoạt động: Thảo luận lớp — Bạn có quyền kiểm soát tiền của chính mình không?

10.3 Lợi ích của Bitcoin

10.4 Một tương lai được trao quyền

Hoạt động: Thảo luận lớp — Quan điểm của bạn đã thay đổi như thế nào?

Tại sao Bitcoin?

10.0 Giới thiệu



Bitcoin không chỉ là một loại tiền tệ; đó là một cuộc cách mạng trả lại quyền lực cho người dân, mang đến cho họ hướng vị của sự bình yên và tự do trong một thế giới khát khao quyền lực.

My First Bitcoin



Trong chương kết này, chúng ta sẽ tổng kết những bài học đã học được suốt hành trình, đặt ra và thảo luận một số câu hỏi quan trọng, đồng thời khám phá tương lai của Bitcoin.

Bitcoin không chỉ là một công nghệ; nó là một dạng mạng lưới vận hành một loại tiền mới với nguồn cung cố định, không thể thay đổi bởi bất kỳ cá nhân hay tổ chức nào. Nhân loại chưa từng có một hình thức tiền tệ nào với nguồn cung cố định và không bị kiểm soát tập trung. Nếu được sử dụng rộng rãi, Bitcoin sẽ là công cụ mở ra một phong trào thay đổi tích cực, có khả năng cải thiện cuộc sống của mọi người trên toàn thế giới. Nó đại diện cho một cuộc cách mạng hòa bình hướng đến tự do và công bằng chung, tạo ra những cơ hội mới cho nhân loại bằng cách xây dựng một hệ thống tiền tệ toàn cầu và chia sẻ.

Là một hệ thống toàn cầu phi tập trung, Bitcoin mang lại tự do tài chính lớn hơn, chuyển giao quyền lực từ số ít sang số nhiều. Nó cung cấp một nền tảng an toàn, chống kiểm duyệt để lưu trữ và chuyển giá trị, giúp cá nhân tự làm chủ tài sản và bảo vệ sức mua của mình. Điều này đặc biệt quan trọng trong bối cảnh kinh tế hiện nay đầy biến động, khi hệ thống tài chính truyền thống đang đổi mới với những thách thức chưa từng có.

Hoạt động: Xem video

Khả năng tạo ra thay đổi tích cực là vô cùng to lớn, đó là lý do vì sao chúng tôi mời bạn xem video này để tìm hiểu thêm.



Tiếp theo, chúng ta sẽ tìm hiểu một dạng tiền kỹ thuật số khác gọi là Tiền kỹ thuật số của Ngân hàng Trung ương (CBDC) và đánh giá xem nó giống và khác Bitcoin như thế nào.

10.1 Tiền kỹ thuật số của ngân hàng trung ương (CBDC) là gì và ai kiểm soát chúng?

Tiền kỹ thuật số của ngân hàng trung ương (CBDC) là phiên bản kỹ thuật số của tiền pháp định truyền thống. CBDC tuân theo các quy tắc giống như tiền pháp định, trong đó một cơ quan trung ương như chính phủ có thể tạo ra thêm nguồn cung, từ đó làm giảm sức mua của người dân. Tuy nhiên, CBDC còn trao cho chính phủ những công cụ mới và mạnh mẽ để kiểm soát cách mà người dân trên toàn thế giới sử dụng đồng tiền đó.

Theo nghiên cứu của Tổ chức Nhân quyền (Human Rights Foundation, viết tắt là HRF), có 119 trong tổng số 193 chính phủ trên thế giới đang xem xét, thử nghiệm hoặc triển khai CBDC.

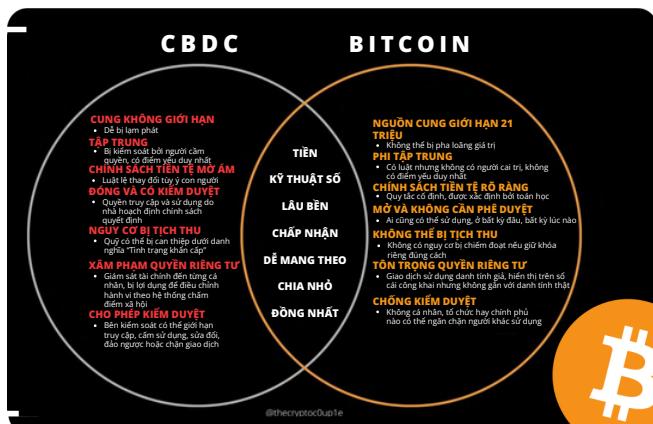
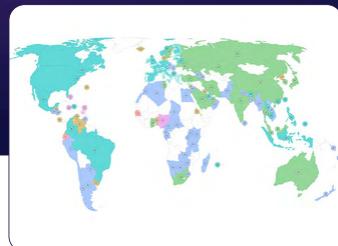
Bạn có thể kiểm tra xem quốc gia của mình có đang thử nghiệm CBDC hay không trên công cụ theo dõi CBDC của Human Rights Foundation tại <https://cbdctracker.hrf.org/home> hoặc <https://cbdctracker.org/>

Vậy, điều gì khiến CBDC khác với tiền pháp định thông thường ngoài việc là tiền kỹ thuật số? Điều quan trọng cần hiểu là, không giống như tiền pháp định dưới dạng tiền giấy hay tiền xu, CBDC cho phép chính phủ theo dõi và kiểm soát mọi giao dịch một cách kỹ thuật số trên toàn cầu. Điều này có nghĩa là chính phủ có thể chặn một số giao dịch nhất định hoặc thậm chí đóng băng toàn bộ tài khoản của bạn nếu họ không hài lòng với bạn hoặc cách bạn sử dụng tiền của mình.

Ví dụ, hãy tưởng tượng bạn muốn gửi tiền cho một người thân ở một quốc gia đang cần hỗ trợ, nhưng chính phủ của bạn lại từ chối giao dịch vì họ không đồng tình với chính quyền của quốc gia đó. Hoặc hãy tưởng tượng bạn đi đến cửa hàng để mua thứ gì đó mình thích, nhưng không thể thanh toán vì bạn đã bày tỏ quan điểm cá nhân trên mạng xã hội.

CBDC trao cho các chính phủ quyền lực không giới hạn trong việc kiểm soát cách tiền được sử dụng trên toàn thế giới, hạn chế khả năng chi tiêu theo ý muốn của từng cá nhân. Một số người thậm chí cho rằng CBDC có thể cho phép các chính phủ hùng mạnh thực thi những chính sách độc tài trên quy mô toàn cầu chỉ bằng một cái nón nút, mà không cần đến lực lượng thực thi pháp luật con người.

Cả CBDC và Bitcoin đều là tiền kỹ thuật số, nhưng ngoài điểm chung đó, chúng đại diện cho hai hình thức tiền tệ hoàn toàn khác nhau với triết lý riêng biệt, dẫn đến những tác động rất khác nhau đối với nhân loại.



Tại sao Bitcoin?

10.2 Triết lý của Bitcoin

Trong Chương 6 và 9, chúng ta đã tìm hiểu rằng những người vận hành node góp phần bảo vệ các quy tắc của Bitcoin. Đây là một điều rất quan trọng, vì lần đầu tiên trong lịch sử, những người bình thường như chúng ta có thể tham gia vào một hệ thống giúp đảm bảo các quy tắc của hệ thống tiền tệ được duy trì. Những quy tắc này bao gồm việc nguồn cung tiền là có giới hạn, và không có bất kỳ cá nhân hay tổ chức nào có thể tự ý thay đổi chúng. Đây là một cơ hội đặc biệt để mọi người cùng nhau giữ cho tiền tệ của chúng ta an toàn và đáng tin cậy.

Triết lý của Bitcoin xoay quanh sự trao quyền, tự do, độc lập tài chính, tư duy phản biện và quan điểm rằng tất cả chúng ta đều nên có tiếng nói trong việc lựa chọn và xác định các quy tắc của hệ thống mà mình sử dụng. Khác với hệ thống tiền pháp định được kiểm soát bởi các tổ chức quyền lực trung ương, Bitcoin vận hành trên một mạng lưới nơi không có bất kỳ bên nào nắm toàn quyền kiểm soát. Điều này có nghĩa là, không giống như các loại tiền khác như CBDC, không ai có thể tước đoạt tài sản của bạn hay ngăn bạn sử dụng tiền theo cách mà bạn muốn.

Trong thế giới tiền pháp định, người có nhiều tài sản hơn thường đồng nghĩa với việc có nhiều quyền lực và khả năng kiểm soát hơn. Ngược lại, Bitcoin hoạt động theo cách trao quyền cho tất cả mọi người. Đây là một nỗ lực tập thể, nơi mỗi người, dù giàu hay nghèo, đều đóng vai trò quan trọng trong hệ thống. Hãy tưởng tượng đó là một sức mạnh chung, nơi quy mô tài chính của bạn không tự động quyết định khả năng kiểm soát hệ thống. Bitcoin được xây dựng trên những quy tắc bất biến và trong sự hài hòa đó, chính con người, chứ không phải một nhóm nhỏ có quyền lực, đang làm chủ hệ thống. Tất cả chúng ta đang cùng nhau vận hành như một cộng đồng bền bỉ, dẫn dắt hướng đi của Bitcoin mà không cần bất kỳ một quyền lực trung ương nào ra lệnh.

Trong khi ở hệ thống tiền pháp định, những người có quyền lực đặt ra luật lệ, thì trong hệ sinh thái Bitcoin, chính sức mạnh tập thể của các cá nhân mới duy trì mạng lưới. Không một thực thể nào, dù giàu có đến đâu, có thể quyết định hướng đi của hệ sinh thái Bitcoin. Đây là sự đảo ngược hoàn toàn so với mô hình quyền lực truyền thống, nơi sức mạnh của hệ thống không nằm trong tay một số ít người mà nằm trong sức mạnh chung của tất cả những người tham gia.

Ý tưởng cốt lõi là xây dựng một hệ thống an toàn, minh bạch và công bằng, nơi mọi người đều có cơ hội tiếp cận đồng tiền toàn cầu một cách bình đẳng.

Hoạt động: Thảo luận lớp — Bạn có quyền kiểm soát tiền của chính mình không?

- 1 Tiền có phải là một nhu cầu thiết yếu và quyền cơ bản của con người không? Tại sao?
- 2 Nếu bạn không thể chi tiêu tiền theo ý muốn, gửi tiền cho người bạn muốn, hoặc mang tiền theo khi chuyển sang quốc gia khác, liệu số tiền đó có thật sự là của bạn không? Tại sao?
- 3 Tại sao việc đổi chác không còn được sử dụng nữa? Vấn đề của việc trùng khớp nhu cầu là gì?
- 4 Sự kiện lịch sử nào để lại ấn tượng sâu sắc nhất đối với bạn? Tại sao việc hiểu về cú sốc Nixon lại quan trọng và có ý nghĩa gì với tất cả mọi người ngày nay?
- 5 Tiền có nguồn cung cố định khác gì so với tiền pháp định truyền thống?

- 6 Bitcoin được tạo ra khi nào, bởi ai, với mục đích gì, và mục đích đó định nghĩa như thế nào về khái niệm hệ thống phi tập trung?
- 7 Sự khác biệt giữa ví lưu ký và ví phi lưu ký là gì? Bạn thích loại ví nào nhất?
- 8 Bạn hiểu gì về Lightning Network? Bạn sẽ sử dụng nó cho loại giao dịch nào?
- 9 Tại sao việc vận hành node riêng lại góp phần hỗ trợ mạng lưới?
- 10 Việc kiểm soát tiền của chính mình giúp bạn trao quyền cho bản thân trong cuộc sống hàng ngày và lập kế hoạch tương lai như thế nào?
- 11 Tự do tài chính có thể nâng cao khả năng đóng góp tích cực cho cộng đồng hoặc xã hội của bạn bằng những cách nào?

10.3 Lợi ích của Bitcoin

"Hyperbitcoinization" (siêu Bitcoin hóa) là một tương lai lý thuyết, trong đó Bitcoin trở thành hệ thống tiền tệ toàn cầu chiếm ưu thế. Điều này có nghĩa là Bitcoin sẽ được mọi người sử dụng ở khắp mọi nơi và cho mọi mục đích — từ mua cà phê, thanh toán hóa đơn đến mua nhà đất.

Sự quan tâm ngày càng tăng đối với Bitcoin từ cá nhân, doanh nghiệp, quốc gia và chính phủ cho thấy tiềm năng ảnh hưởng lớn của việc Bitcoin được sử dụng rộng rãi đối với kinh tế và xã hội. Dưới đây là một số lợi ích của thế giới siêu Bitcoin hóa:

Một tương lai tự chủ:

1 Tương lai tự chủ là khi mỗi cá nhân trên toàn thế giới có toàn quyền kiểm soát danh tính kỹ thuật số và tài sản của chính mình. Điều này có thể dẫn đến sự bao trùm tài chính rộng hơn, tăng cường tự do, quyền riêng tư và an ninh, từ đó góp phần nâng cao sự thịnh vượng, dư dả và hạnh phúc chung của con người.

Công cụ cất trữ giá trị đáng tin cậy:

Tính khan hiếm kỹ thuật số của Bitcoin khiến nó trở thành một công cụ cất trữ giá trị đáng tin cậy, từ đó có thể khuyến khích nhiều người sử dụng nó như một phương tiện tiết kiệm cho tương lai.

Thay đổi chính sách tiền tệ:

3 Nếu Bitcoin được sử dụng rộng rãi, nó có thể làm mất đi khả năng kiểm soát nguồn cung tiền của chính phủ thông qua các công cụ chính sách tiền tệ truyền thống. Việc áp dụng Bitcoin đại trà có thể tăng sức mua của người dân và khuyến khích xã hội hướng đến những hoạt động có mức độ ưu tiên thời gian thấp hơn.

Tăng cường minh bạch và khả năng truy vết:

4 Bản ghi không thể giả mạo và không thể thay đổi của tất cả các giao dịch trên blockchain có thể tăng cường tính minh bạch và trách nhiệm giải trình trong nhiều ngành và lĩnh vực khác nhau. Hiện nay, các tổ chức quyền lực có khả năng di chuyển hàng nghìn tỷ đô la trên toàn thế giới mà không có sự minh bạch rõ ràng về nơi các quỹ này được sử dụng hay cách chúng được quản lý. Bằng cách cung cấp một bản ghi tài chính mở và có thể kiểm chứng, Bitcoin có thể đảm bảo rằng dòng vốn trở nên minh bạch hơn và dễ tiếp cận hơn với công chúng.

Tại sao Bitcoin?

5

Cuộc Cách Mạng Trong Thị Trường Chuyển Tiền:

Thị trường chuyển tiền bao gồm việc chuyển quỹ từ người gửi sang người nhận, thường xuyên qua biên giới quốc tế. Mặc dù chi phí chuyển tiền đã giảm, nhưng so với chuyển khoản nội địa thì vẫn khá đắt, đặc biệt với những khoản tiền nhỏ. Lightning Network cung cấp các giao dịch nhanh chóng và chi phí thấp, rất phù hợp cho thị trường chuyển tiền và giải quyết những vấn đề như chi phí cao, thời gian thanh toán chậm, và giới hạn giờ làm việc của các đơn vị chuyển tiền.

6

Năng Lượng Dồi Dào:

Khi có nhiều năng lượng với chi phí hợp lý, xã hội phát triển tốt và nhiều ngành công nghiệp cũng như cộng đồng có thể đáp ứng nhu cầu ngày càng tăng về điện năng cho nhà cửa, doanh nghiệp và công nghệ mới. Việc khai thác Bitcoin khuyến khích các thợ mỏ sử dụng lượng năng lượng dư thừa mà thường bị lãng phí từ các nguồn năng lượng bền vững như năng lượng mặt trời, gió và thủy điện. Các thợ mỏ Bitcoin sử dụng năng lượng dư thừa này để tạo ra bitcoin mới qua hoạt động khai thác, bảo vệ mạng lưới, đồng thời cung cấp lượng điện dư thừa trở lại lưới điện để xã hội sử dụng khi cần thiết.

10.4 Một tương lai được trao quyền

Bitcoin là tiền

Tiền giúp con người giao tiếp để xác định những hoạt động, hàng hóa và dịch vụ nào là quan trọng nhất trong xã hội. Như chúng ta đã thấy trong khóa học này, khi tiền bị kiểm soát bởi các cơ quan tập trung, nó sẽ bị thao túng.

Một trong những sai lầm mà nhân loại liên tục lặp lại trong suốt lịch sử là việc thao túng tiền tệ, điều này gây ảnh hưởng tiêu cực đến cá nhân, gia đình, doanh nghiệp, chính phủ và cuối cùng là sự thịnh vượng toàn cầu của con người.

Bằng cách đưa quyền kiểm soát tiền ra khỏi tay các bên tập trung và thay vào đó sử dụng một loại tiền có nguồn cung cố định mà không bên nào có thể thay đổi, chúng ta đang tạo ra một thế giới khác — một thế giới mà chúng ta không cần phải tin rằng con người sẽ làm điều đúng đắn, mà là nơi con người không thể làm điều sai trái.

Đây là một thế giới hoàn toàn khác biệt.

Và bạn, học viên thân mến, có thể là một phần trong việc xây dựng thế giới đó. Bằng cách sử dụng Bitcoin, vận hành node của riêng mình và giúp người khác hiểu rõ hơn về tương lai của tiền tệ, bạn đang bỏ phiếu cho một thế giới khác biệt.

Hoạt động: Thảo luận cuối khoá — Quan điểm của bạn đã thay đổi như thế nào?

Vui lòng trả lời năm câu hỏi dưới đây:

Tại sao chúng ta cần tiền?

Tiền là gì?

Tại sao Bitcoin?

Ai kiểm soát tiền?

Điều gì tạo nên “giá trị” của tiền?

Ghi lại các câu hỏi được học viên đặt ra và được chọn trong Chương 1, kèm theo câu trả lời.

- 1** Quay lại hoạt động đầu tiên trong Chương 1 và so sánh câu trả lời mới của bạn với câu trả lời cũ.
- 2** Hãy so sánh và thảo luận các câu hỏi và câu trả lời ban đầu. Có điều gì đã thay đổi không?
- 3** Tự hỏi bản thân câu hỏi cuối cùng này: Bước tiếp theo Bitcoin là gì? Và tôi có thể sử dụng kiến thức mới này để trao quyền cho bản thân như thế nào?



Nếu bạn đã sẵn sàng bước tiếp, hãy khám phá các tài liệu bổ sung trong phần tiếp theo, nơi chúng tôi đã lựa chọn những nguồn học tốt nhất để bạn tiếp tục tìm hiểu và đạt được thành công.

Tài nguyên bổ sung

1. Tại sao nên sử dụng Bitcoin?

- a "The Bullish Case for Bitcoin" (Lập luận tích cực về Bitcoin) của Vijay Boyapati:
Bài viết này trình bày lý do tại sao Bitcoin là một tài sản có giá trị và tại sao nó có tiềm năng trở thành đồng tiền toàn cầu thống trị. Tác giả phân tích các khía cạnh kỹ thuật và kinh tế của Bitcoin, làm nổi bật cơ hội đầu tư hấp dẫn.
- b "Why Bitcoin Matters" (Tại sao Bitcoin quan trọng) của Aleks Svetski (1 giờ):
Video này nói về tầm quan trọng của Bitcoin như một tài sản kỹ thuật số phi tập trung và cách nó có thể ảnh hưởng đến hệ thống tài chính hiện tại. Diễn giả khám phá tiềm năng của Bitcoin trong việc mang lại tự do tài chính cho mọi người trên toàn thế giới.
- c "Why Bitcoin" (Tại sao Bitcoin) của Wiz:
Bài viết này cung cấp cái nhìn tổng quan về những lợi ích của việc sử dụng Bitcoin như một loại tiền tệ và cất trữ giá trị. Nội dung nhấn mạnh tính phi tập trung của Bitcoin và cách mà nó mang lại tự do tài chính lớn hơn cũng như sự an toàn cao hơn.

2. Bitcoin là gì?

- a "How Bitcoin Works under the Hood" (Cách Bitcoin hoạt động bên trong) của CuriousInventor:
<https://www.youtube.com/watch?v=Lx9zgZCMqXE> Video này cung cấp giải thích chi tiết về các khía cạnh kỹ thuật của Bitcoin và cách nó hoạt động.
- b "What Is Bitcoin" (Bitcoin là gì?) của Greg Walker:
Bài viết này giải thích toàn diện về Bitcoin, bao gồm lịch sử hình thành, công nghệ nền tảng và cách nó khác biệt so với các loại tiền tệ truyền thống.
- c "Bitcoin - The Genesis" (Bitcoin - Khởi nguồn) by RT (30 phút):
Video này nói về sự ra đời và những ngày đầu của Bitcoin. Nội dung khám phá động cơ của người sáng lập bí ẩn Satoshi Nakamoto và cách ý tưởng về Bitcoin đã phát triển.

3. Tìm Hiểu Thêm:

- a "The Bitcoin Standard" (Tiêu Chuẩn Bitcoin) (1 giờ 40 phút):
Sách nói này khám phá bối cảnh kinh tế và lịch sử dẫn đến sự ra đời của Bitcoin. Nội dung đề cập đến những lợi ích của một loại tiền tệ phi tập trung và tiềm năng để Bitcoin trở thành một tiêu chuẩn toàn cầu.
- b "Intro to Bitcoin Austrian Thought" (Giới thiệu về Bitcoin và Tư tưởng Áo) (1 giờ):
Bài giảng âm thanh này trình bày về Trường phái Kinh tế Áo và mối liên hệ của nó với khái niệm Bitcoin. Nội dung cung cấp cái nhìn sâu sắc về các nguyên lý kinh tế đằng sau Bitcoin và cách mà Bitcoin phù hợp với tư tưởng kinh tế Áo.
- c "Bitcoin Babies"
Tác giả Naomi Wambui -<https://bitcoinbabies.com/>
Twitter: @btcbabies - @ngachanaomi1
Một tài liệu PDF miễn phí nhằm trao quyền cho các bà mẹ với kiến thức thiết yếu về dinh dưỡng, Bitcoin, và sức khỏe tinh thần tổng thể.
- d **BTC Sessions**
Kênh YouTube giáo dục chỉ về Bitcoin với các hướng dẫn và bài học hữu ích:
<https://www.youtube.com/@BTCSessions>

4. Khóa học:

- a **Summer of Bitcoin**
<https://www.summerofbitcoin.org/>: Một chương trình thực tập mùa hè trực tuyến toàn cầu tập trung giới thiệu sinh viên đại học về phát triển và thiết kế mã nguồn mở của Bitcoin.

b Chaincode Labs

<https://learning.chaincode.com/#FOSS>: Các khóa học trực tuyến và chương trình lưu trú giúp sinh viên học các kỹ năng cần thiết để phát triển giao thức Bitcoin.

c Saylor Academy

Giáo dục miễn phí đa ngành:
<https://www.saylor.org/>

5. Tác giả quan trọng

- a Alex Gladstein: *Kiểm tra đặc quyền tài chính của bạn*
- b Alex Swan: (*Liệu pháp gấp gáp thực tế: Quan điểm, đặc điểm và ứng dụng*)
- c Amanda Cavalieri: *Bitcoin và Giấc mơ Mỹ: Công nghệ tiền tệ mới vượt lên sự chia rẽ chính trị*
- d Anita Posch: *Học Bitcoin: Trở nên tự chủ tài chính*
- e Eric Yakes: Thuộc tính thứ 7: Bitcoin và cuộc cách mạng tiền tệ

- f Jeff Booth: *Giá của ngày mai: Tại sao giảm phát là chìa khóa cho tương lai thịnh vượng*
- g Jimmy Song: *Cuốn sách nhỏ về Bitcoin: Tại sao Bitcoin quan trọng với tự do, tài chính và tương lai của bạn*
- h Nik Bhatia: *Tiền nhiều lớp: Từ vàng và đô la đến Bitcoin và tiền kỹ thuật số của ngân hàng trung ương*
- i Robert Breedlove: *Ôn Trời có Bitcoin: Sự sáng tạo, tha hóa và cùu chuộc của tiền*
- j Lyn Alden: *Tiền bị vỡ vụn*

6. Tác Giả Được Trích Dẫn

a Curious Inventor:

<https://www.youtube.com/@CuriousInventor>

b Anil Patel:

Twitter: @anilsaidso

7. Tài Nguyên Khác:

- ❶ **Bitcoin.org:** Trang web chính thức của giao thức Bitcoin.
- ❷ **Bitcointalk.org:** Bitcointalk là một diễn đàn nơi người dùng có thể thảo luận về các chủ đề liên quan đến Bitcoin, đặt câu hỏi và chia sẻ thông tin. Đây là nơi tuyệt vời để học hỏi từ những người đam mê và chuyên gia về Bitcoin.
- ❸ **Bitcoincore.org:** Đây là phần mềm gốc của Bitcoin và vẫn được nhiều người dùng cũng như nhà phát triển sử dụng rộng rãi. Nó cung cấp bộ công cụ mạnh mẽ để tương tác với mạng Bitcoin và xây dựng các ứng dụng Bitcoin.
- ❹ **Bitcoinwiki.org:** Đây là một nguồn tài nguyên do cộng đồng đóng góp, cung cấp hướng dẫn toàn diện về mọi thứ liên quan đến Bitcoin, từ các khía cạnh kỹ thuật cho đến lịch sử và các trường hợp sử dụng.
- ❺ **Bitcoinmagazine.com:** Một ấn phẩm trực tuyến đưa tin tức và phân tích về Bitcoin và các loại tiền mã hóa khác. Đây là cách tuyệt vời để cập nhật những diễn biến mới nhất trong hệ sinh thái Bitcoin.
- ❻ **Bitcoin.Design:** Kho tài nguyên mã nguồn mở chứa các tệp thiết kế liên quan đến Bitcoin, bao gồm hình minh họa, trang web, mẫu và biểu tượng.
- ❼ **Yzer:** <https://yzer.io/> Ứng dụng giáo dục Bitcoin đơn giản trên điện thoại. Học về Bitcoin, tài chính, kinh tế và nhận phần thưởng bằng Satoshis.

❽ **NOSTR:** <https://nostr.com/> - Mạng xã hội nơi bạn thuật sự sở hữu dữ liệu cá nhân của mình.

❾ **Simple X:** <https://simplex.chat/> - Giao thức ứng dụng riêng tư, phi tập trung.

❿ **Set up a Bitcoin Node:** Tự làm với Raspberry Pi bởi Keith Mukai: https://github.com/kdmukai/raspb4_bitcoin_node_tutorial?ab=readme-ov-file

❻ **Cách chọn ví Bitcoin:** <https://bitcoin.org/en/choose-your-wallet> - Sử dụng kiến thức bạn đã học để chọn ra ví phù hợp với nhu cầu của mình.

❻ **BitcoinIcons.com:** <https://bitcoinicons.com/> - Bộ sưu tập biểu tượng Bitcoin miễn phí.

❻ **Bitcoin Dành Cho Doanh Nghiệp Địa Phương:** <https://bitcoinforlocalbusiness.com/> - Bộ tờ rơi giúp bạn chia sẻ giá trị của Bitcoin với các doanh nghiệp địa phương yêu thích.

❻ **Mempool.Space:** <https://mempool.space/> - Dự án mã nguồn mở hiển thị dữ liệu Mempool và các biểu đồ liên quan đến Lightning Network.

Khái niệm chính của chương

Chương 1:

Giới thiệu về khóa học:

Khám phá mục tiêu và kỳ vọng của khóa học Văn bằng Bitcoin.

Hoạt động phản tư — Định nghĩa về tiền:

Tham gia một bài tập phản tư bằng cách đưa ra năm câu trả lời cho các câu hỏi quan trọng về tiền.

Thảo luận lớp — Tại sao chúng ta cần tiền?

- Tham gia thảo luận toàn lớp để khám phá nhu cầu thiết yếu của tiền.
- Chia sẻ và so sánh góc nhìn cá nhân về tầm quan trọng của tiền.
- Xây dựng nền tảng để hiểu rõ vai trò của tiền trong các hệ thống kinh tế.

Chương 2:

Hiểu về tiền:

- Khám phá định nghĩa cơ bản và khái niệm về tiền.
- Thảo luận các quan điểm đa dạng trong lớp để hiểu rõ tính đa chiều của tiền.

Tâm lý học về tiền:

- Hiểu các khía cạnh tâm lý của tiền, bao gồm sự khan hiếm, ưu tiên thời gian và đánh đổi.
- Tham gia hoạt động “Ưu tiên thời gian” để liên hệ các yếu tố tâm lý với các tình huống thực tế.

Chức năng, đặc tính và các loại hình:

- Tìm hiểu sâu về chức năng, đặc tính và các loại tiền.
- Nhận thức được tầm quan trọng của những yếu tố này trong việc xác định và sử dụng tiền.

Chương 3:

Giới thiệu về lịch sử và sự tiến hóa của tiền:

Khám phá lịch sử và quá trình tiến hóa của tiền. Hiểu cách các hình thức trao đổi cổ đại dẫn đến sự phát triển của tiền tệ mà chúng ta sử dụng ngày nay.

Cuộc cách mạng tiền tệ kỹ thuật số:

- Khám phá đỉnh cao hiện nay của sự tiến hóa tiền tệ — tiền kỹ thuật số.
- Hiểu cách tiền kỹ thuật số chỉ tồn tại dưới dạng điện tử, cho phép các giao dịch nhanh chóng và chi phí thấp trên toàn cầu.
- Tìm hiểu vai trò quan trọng của Bitcoin trong việc giải quyết những thách thức ban đầu của tiền kỹ thuật số, giúp nó sẵn sàng cho việc sử dụng trên toàn thế giới.

Sự tiến hóa của tiền tệ:

Tìm hiểu quá trình chuyển đổi từ các hình thức tiền cổ đại như vỏ sò, hạt cườm sang tiền kim loại và tiền giấy. Theo dõi hành trình từ tiền giấy đến thẻ nhựa, khám phá sự tiến hóa của tiền tệ qua các thời kỳ lịch sử.

Hoạt động trò chơi đổi chác:

Tham gia trải nghiệm trò chơi đổi chác thực tế để hiểu rõ những thách thức của việc trao đổi trực tiếp và nhận thức được sự cần thiết của một hệ thống hiệu quả hơn.

Chương 4:

Nguồn gốc tiền fiat:

Khám phá nguồn gốc của tiền fiat qua cái nhìn tổng quan lịch sử, hiểu cách thức nó trở thành hình thức tiền tệ chiếm ưu thế.

Hoạt động ngân hàng dự trữ một phần:

Tham gia vào hoạt động Ngân hàng dự trữ một phần để hiểu cách hệ thống này vận hành, làm nổi bật sự phụ thuộc vào nợ và những tác động đối với nền kinh tế rộng lớn hơn.

Chương 5:

Sức mua giảm sút:

Tìm hiểu khái niệm lạm phát tiền tệ và tác động của nó đến sức mua. Tham gia hoạt động 'Tác động của Lạm phát — Hoạt động Đầu giá' để trực tiếp trải nghiệm những ảnh hưởng này.

Hoạt động hậu quả của hệ thống tiền pháp định:

Tham gia hoạt động 'Hậu quả của hệ thống tiền pháp định' nhằm làm sáng tỏ những tác động rộng lớn hơn của khung tiền tệ hiện tại.

Tiền tệ kỹ thuật số của ngân hàng trung ương (CBDC):

Khám phá bối cảnh đang phát triển của các loại tiền kỹ thuật số do ngân hàng trung ương phát hành (CBDC) và tiềm năng ảnh hưởng của chúng đến tương lai của tiền tệ.

Chương 6:

Satoshi Nakamoto và sự ra đời của Bitcoin:

Tìm hiểu về nhân vật bí ẩn Satoshi Nakamoto và câu chuyện khởi nguồn của Bitcoin, qua đó hiểu rõ những động lực ban đầu thúc đẩy sự phát triển của đồng tiền này.

Hoạt động trên lớp — Xây dựng Đồng thuận:

Tham gia hoạt động Xây dựng đồng thuận trong mạng ngang hàng để hiểu rõ hơn cách thức đạt được sự đồng thuận trong mạng lưới Bitcoin.

Chấp nhận trách nhiệm cá nhân:

Nhấn mạnh khái niệm trách nhiệm cá nhân trong bối cảnh Bitcoin, khuyến khích hiểu rõ vai trò và trách nhiệm của mỗi cá nhân trong hệ sinh thái phi tập trung.

Hệ thống tiền pháp định

Hiểu rõ các khía cạnh cơ bản của hệ thống tiền pháp định, bao gồm bản chất là một hệ thống tiền tệ theo nghị định, vai trò của ngân hàng dự trữ một phần, và các tác nhân chính kiểm soát hệ thống này.

Gánh nặng nợ toàn cầu và bất bình đẳng xã hội:

Khám phá tác động kép của gánh nặng nợ toàn cầu và tình trạng bất bình đẳng xã hội. Nhận diện những hậu quả đối với cá nhân và xã hội, đặc biệt là sự mất giá sức mua và khoảng cách giàu nghèo ngày càng mở rộng.

Phong trào Cypherpunk và tính phi tập trung:

Tìm hiểu câu chuyện của các Cypherpunk và động lực thúc đẩy họ theo đuổi một loại tiền tệ phi tập trung. Phân biệt giữa hệ thống tập trung và phi tập trung, đồng thời rút ra những bài học từ lịch sử ngắn gọn của các loại tiền kỹ thuật số.

Cách Bitcoin hoạt động:

Tìm hiểu về cơ chế vận hành của Bitcoin, bao gồm Cơ Chế Đồng Thuận Nakamoto. Nhận diện các nhân tố chính trong mạng lưới Bitcoin như thợ đào, nút mạng, người dùng, nhà phát triển và các dự án, đồng thời nắm bắt mối quan hệ hợp tác giữa họ.

Bitcoin như tiền kỹ thuật số có giá trị thực:

Khám phá vai trò của Bitcoin như một loại tiền kỹ thuật số có giá trị thực, thảo luận về quá trình phát triển, các chức năng và đặc tính của nó, và tham gia thảo luận lớp về việc liệu Bitcoin có đáp ứng tiêu chuẩn của một loại tiền vững chắc hay không.

Khái niệm chính của chương

Chương 7:

Giao dịch ngang hàng:

Tham gia vào các giao dịch phi tập trung để trải nghiệm những nguyên tắc cốt lõi của việc trao đổi Bitcoin.

Thiết lập ví Bitcoin:

Tìm hiểu các bước cơ bản để tải về, tạo khóa và sao lưu ví Bitcoin nhằm thực hiện giao dịch một cách an toàn.

Tiết kiệm và tự tìm hiểu:

Hiểu việc tiết kiệm bằng Bitcoin như một phương thức lưu trữ giá trị và tầm quan trọng của việc tự nghiên cứu để đưa ra quyết định sáng suốt.

Các loại ví Bitcoin:

Phân biệt giữa ví mã nguồn mở, mã nguồn đóng, ví lưu ký và không lưu ký, và hiểu vai trò của khóa trong bảo mật.

Mua Bitcoin:

Tìm hiểu các phương pháp như giao dịch ngang hàng và sàn giao dịch, cùng với các vấn đề liên quan đến quyền riêng tư trong quy trình KYC.

Chương 8:

Giới thiệu về Lightning Network:

Nhận biết sự phát triển của Bitcoin thông qua các công nghệ như Lightning Network, giúp nâng cao khả năng của nó.

Cài đặt ví Lightning:

Tìm hiểu các bước cần thiết để thiết lập ví Lightning của Bitcoin, giúp thực hiện giao dịch nhanh hơn và dễ mở rộng hơn.

Hoạt động thực hành:

Tham gia một cuộc đua tiếp sức sử dụng ví Lightning để hiểu một cách sinh động về giao dịch trên Lightning Network.

Các loại ví Lightning:

Phân biệt giữa ví Lightning mã nguồn mở, mã nguồn đóng, ví lưu ký và ví không lưu ký để phù hợp với các sở thích khác nhau của người dùng.

Giao dịch Lightning:

Tìm hiểu quy trình gửi và nhận giao dịch Lightning, nhấn mạnh tốc độ và hiệu quả của Lightning Network.

Chương 9:

Số cái Bitcoin:

Nắm bắt khái niệm về số cái phi tập trung được vận hành bởi các nút mạng và thợ đào, giúp đảm bảo tính minh bạch và bảo mật cho hệ thống.

Mô hình UTXO:

Hiểu rõ mô hình "đầu ra giao dịch chưa sử dụng" (UTXO) như một yếu tố cốt lõi trong quy trình giao dịch của Bitcoin.

Khóa công khai và khóa riêng:

Tìm hiểu vai trò của bảo mật mật mã trong các giao dịch Bitcoin thông qua cấp khóa công khai và khóa riêng, kèm theo một hoạt động minh họa cơ chế băm SHA-256.

Các nút và thợ đào Bitcoin:

Tìm hiểu vai trò của các nút mạng và thợ đào trong việc duy trì mạng lưới Bitcoin, bao gồm các khía cạnh như phát hành, sự khan hiếm, cơ chế giảm một nửa và độ khó khai thác.

Cách thức hoạt động của giao dịch Bitcoin:

Khám phá toàn bộ vòng đời của một giao dịch Bitcoin, từ người gửi, người nhận, đến các nút mạng, thợ đào và mempool, kèm theo một hoạt động chuyên biệt về mempool.

Chương 10:



Triết lý nền tảng của Bitcoin:

Khám phá triết lý cốt lõi đứng sau sự ra đời của Bitcoin, hiểu cách mà nó xuất hiện như một phản ứng trước các thách thức kinh tế, tập trung vào tác động của nó đối với tự do tài chính và sự khác biệt so với các loại tiền tệ truyền thống.



Tương lai của Bitcoin:

Tìm hiểu về tiềm năng phát triển và những bước tiến trong tương lai của Bitcoin với vai trò là một loại tiền tệ kỹ thuật số mang tính cách mạng.



Suy ngẫm về văn bằng:

Tóm tắt những điểm chính rút ra từ Văn bằng Bitcoin, khuyến khích học viên suy ngẫm về hành trình học tập và những hiểu biết đã tích lũy được.

Các hoạt động bao gồm xem một video về “Tại sao Bitcoin?” và quay lại các câu hỏi trong Chương 1 để tự đánh giá sự phát triển trong quá trình hiểu biết của bản thân.

Bảng thuật ngữ

Tấn công 51%: Một kiểu tấn công vào mạng lưới blockchain khi một cá nhân hoặc nhóm kiểm soát phần lớn sức mạnh tính toán của mạng. Điều này cho phép họ thao túng giao dịch và có thể gây gián đoạn cho mạng lưới.

Mùa Altcoin: Giai đoạn các loại tiền mã hóa thay thế (altcoin) tăng giá mạnh, thường do sự quan tâm và chấp nhận ngày càng lớn từ nhà đầu tư.

Altcoin: Các loại tiền mã hóa kỹ thuật số không bao gồm Bitcoin.

Hoán đổi nguyên tử (Atomic Swap): Hình thức trao đổi ngang hàng giữa hai loại tiền mã hóa mà không cần đến sàn giao dịch tập trung hoặc bên thứ ba.

Đấu giá: Quá trình bán hàng hóa hoặc tài sản cho người trả giá cao nhất.

Đổi chác: Việc trao đổi hàng hóa và dịch vụ mà không sử dụng tiền.

Giả hàng hóa: Tập hợp các hàng hóa hoặc dịch vụ được dùng để đo lường sự thay đổi chi phí sinh hoạt.

Bitcoin: Một loại tiền kỹ thuật số và hệ thống cho phép mọi người gửi tiền cho nhau mà không cần qua ngân hàng.

Block Explorer: Một công cụ dùng để xem và khám phá blockchain, cho phép người dùng theo dõi từng khối, giao dịch và địa chỉ ví.

Phần thưởng khối: Số bitcoin mới được trao cho thợ đào khi họ thêm một khối mới vào blockchain.

Blockchain: Một bản ghi công khai của tất cả các giao dịch bitcoin đã diễn ra.

BTC: Đơn vị dùng để đo lường bitcoin. Là một loại tiền kỹ thuật số có thể được sử dụng để mua bán hoặc giao dịch.

Kiểm soát vốn: Các hạn chế đối với việc chuyển tiền qua biên giới.

Ngân hàng trung ương (Fed): Tổ chức thuộc chính phủ quản lý chính sách tiền tệ của một quốc gia.

Tập trung: Sự tập trung quyền lực hoặc kiểm soát vào một thực thể duy nhất.

Hệ thống tập trung: Hệ thống mà quyền lực hoặc kiểm soát được tập trung vào một thực thể duy nhất.

Lưu trữ lạnh: Phương pháp lưu trữ bitcoin ngoại tuyến, tránh xa nguy cơ bị tin tặc hoặc các mối đe dọa trực tuyến khác.

Tiền hàng hóa: Những vật phẩm có giá trị vốn có và được sử dụng làm phương tiện trao đổi, chẳng hạn như vàng hoặc bạc.

Xác nhận: Quá trình giao dịch được xử lý bởi mạng lưới và gần như không thể bị đảo ngược. Đây là cách các "thợ đào" dùng phần cứng và phần mềm máy tính để xác minh tính hợp lệ của giao dịch. Người dùng thường được khuyến nghị chờ ít nhất sáu lần xác nhận để tránh rủi ro chi tiêu kép.

Cơ chế đồng thuận: Phương pháp được sử dụng trong công nghệ blockchain để xác thực giao dịch và đảm bảo tính toàn vẹn của blockchain.

Sàn giao dịch tiền mã hóa: Nền tảng cho phép người dùng mua, bán và trao đổi tiền mã hóa với các tài sản khác như tiền pháp định hoặc tiền mã hóa khác.

Ví tiền mã hóa: Một chương trình phần mềm dùng để lưu trữ khóa cá nhân và cho phép người dùng gửi, nhận, cũng như quản lý tiền mã hóa của mình.

Mật mã học: Một nhánh của toán học giúp tạo ra các hệ thống bảo mật.

Làm mất giá tiền tệ (Debasement): Việc làm giảm giá trị của một đồng tiền, thường bằng cách giảm hàm lượng kim loại quý trong đồng xu.

Nợ: Khoản tiền phải trả cho người khác.

Phi tập trung: Việc phân phối quyền lực và kiểm soát trên toàn mạng lưới thay vì tập trung vào một cơ quan trung ương.

Tổ chức tự trị phi tập trung (DAO): Một tổ chức hoặc mạng lưới được quản lý bằng hợp đồng thông minh và vận hành trên blockchain mà không có cơ quan trung ương hay cấu trúc quản lý.

Tài chính phi tập trung (DeFi): Một phong trào trong ngành tiền mã hóa nhằm tạo ra các sản phẩm và dịch vụ tài chính phi tập trung hoạt động trên nền tảng blockchain.

Hệ thống phi tập trung: Hệ thống trong đó quyền lực hoặc kiểm soát được phân phối cho nhiều thực thể khác nhau.

Tài sản kỹ thuật số: Đại diện kỹ thuật số của giá trị có thể được giao dịch hoặc sử dụng làm nơi lưu giữ giá trị, chẳng hạn như bitcoin.

Số cái phân tán: Một cơ sở dữ liệu được phân phối trên mạng lưới các máy tính thay vì lưu trữ tại một vị trí trung tâm.

Trùng khớp nhu cầu: Hiện tượng trong nền kinh tế đổi chác, khi hai bên đều có thứ mà bên kia muốn và cũng muốn thứ mà bên kia có.

Chi tiêu kép: Khi một người cố gắng gửi bitcoin của mình cho hai người nhận khác nhau cùng một lúc.

Giao dịch bụi: Giao dịch gửi một lượng bitcoin rất nhỏ, đến mức không còn mang lại hiệu quả kinh tế.

Bảng thuật ngữ

Tỷ giá hối đoái: Giá trị của một đồng tiền so với đồng tiền khác.

FOMO (Fear Of Missing Out): Nỗi sợ bị bỏ lỡ, thuật ngữ dùng để mô tả cảm giác lo lắng hoặc hối tiếc khi có nguy cơ bỏ lỡ một cơ hội kiếm lời trong thị trường tiền mã hóa.

FUD (Fear, Uncertainty, Doubt): Nỗi sợ hãi, sự không chắc chắn và nghi ngờ, thuật ngữ dùng để chỉ các tin đồn tiêu cực hoặc thông tin gây hoang mang, dẫn đến sự hoảng loạn hoặc suy giảm trên thị trường.

GDP: Tổng sản phẩm quốc nội, tổng giá trị hàng hóa và dịch vụ được sản xuất trong một quốc gia trong một khoảng thời gian nhất định.

Hard Fork: Một thay đổi trong giao thức Bitcoin tạo ra một phiên bản mới của blockchain không tương thích với phiên bản trước đó (ví dụ như Bitcoin Cash).

Ví cứng: Thiết bị vật lý dùng để lưu trữ khóa riêng và quản lý tiền mã hóa, cung cấp mức độ bảo mật cao hơn so với ví phần mềm.

Hàm băm: Một hàm toán học nhận dữ liệu đầu vào với kích thước bất kỳ và trả về một chuỗi ký tự có độ dài cố định, thường được sử dụng trong mật mã học và công nghệ blockchain.

Tỷ lệ băm: Cách đo lường sức mạnh xử lý của mạng Bitcoin.

HODL: Một thuật ngữ trong cộng đồng tiền mã hóa dùng để chỉ việc giữ tiền mã hóa lâu dài thay vì bán hoặc giao dịch ngắn hạn.

Ví nóng: Một loại ví Bitcoin được kết nối với internet, cho phép truy cập và sử dụng Bitcoin một cách dễ dàng.

Nhập khẩu: Hàng hóa và dịch vụ được sản xuất ở nước ngoài và bán trong thị trường trong nước.

Lạm phát: Sự gia tăng mức giá chung của hàng hóa và dịch vụ trong một nền kinh tế.

Phát hành tiền mã hóa lần đầu (ICO): Một phương thức huy động vốn bằng cách bán một loại tiền mã hóa mới cho nhà đầu tư để đổi lấy một loại tiền mã hóa đã được sử dụng rộng rãi hơn, như Bitcoin.

Giao thức lớp 1: Lớp cơ sở của mạng blockchain chịu trách nhiệm về các khía cạnh nền tảng như cơ chế đồng thuận, xác thực giao dịch và lưu trữ dữ liệu.

Giao thức lớp 2: Lớp phụ được xây dựng trên lớp 1 của mạng blockchain, thường dùng để cải thiện khả năng mở rộng, tốc độ và chức năng.

Sổ cái : Bản ghi các giao dịch tài chính.

Lightning Network: Giao thức thanh toán lớp 2 giúp thực hiện các giao dịch bitcoin nhanh hơn và chi phí thấp hơn bằng cách sử dụng các kênh ngoài chuỗi cho các giao dịch nhỏ hơn.

Phương tiện trao đổi: Những vật thể hoặc hệ thống được chấp nhận rộng rãi để trao đổi lấy hàng hóa và dịch vụ.

Cây Merkle: Một cấu trúc dữ liệu dạng cây được sử dụng trong blockchain của Bitcoin để kiểm tra hiệu quả tính toàn vẹn của các tập dữ liệu lớn.

Mỏ đào (Mining Pool): Một nhóm thợ đào hợp tác với nhau để tăng khả năng tìm được khối mới và nhận phần thưởng bằng bitcoin.

Đào coin: Quá trình sử dụng phần cứng máy tính để thực hiện các phép tính toán học cho mạng lưới Bitcoin nhằm xác nhận các giao dịch và tăng cường bảo mật.

Chính sách tiền tệ và tài khóa: Các chính sách của ngân hàng trung ương và chính phủ, tương ứng, nhằm ảnh hưởng đến cung tiền và lãi suất trong nền kinh tế.

Cung tiền: Tổng lượng tiền đang lưu thông trong nền kinh tế.

Ví đa chữ ký (Multisig): Một loại ví yêu cầu nhiều chữ ký hoặc sự phê duyệt từ nhiều bên trước khi giao dịch được thực hiện, nhằm tăng cường bảo mật và kiểm soát.

Đa chữ ký: Một tính năng bảo mật yêu cầu nhiều hơn một khóa riêng để phê duyệt một giao dịch bitcoin.

Mạng lưới: Một nhóm các thực thể được kết nối với nhau.

Mạng lưới nút: Một mạng gồm các máy tính hoặc thiết bị được kết nối với nhau để hỗ trợ và duy trì mạng Bitcoin.

Nút: Một máy tính hoặc thiết bị được kết nối với mạng Bitcoin và tham gia vào việc xác minh và truyền tải các giao dịch.

Non-Fungible Token (NFT): Một loại tài sản kỹ thuật số đại diện cho một vật phẩm độc nhất hoặc có một không hai, thường được sử dụng để đại diện cho các tác phẩm nghệ thuật, đồ sưu tầm hoặc các đối tượng độc đáo khác.

Nonce: Một số ngẫu nhiên được thêm vào đầu khối (block header) để tạo ra một hàm băm (hash) đáp ứng mức độ khó được đặt ra.

Khối mồi côi: Một khối không được đưa vào chuỗi chính của blockchain do bị vô hiệu hóa bởi một chuỗi cạnh tranh dài hơn.

Ví giấy: Một bản in chứa khóa riêng và khóa công khai của người dùng, được sử dụng để lưu trữ và quản lý tiền mã hóa ngoại tuyến.

Mạng ngang hàng (P2P): Một mạng phi tập trung trong đó các thành viên tương tác trực tiếp với nhau mà không thông qua một cơ quan trung gian.

Bảng thuật ngữ

Neo giá (Peg): Tỷ giá cố định giữa hai loại tiền tệ, trong đó một loại tiền tệ được neo giá dựa trên giá trị của loại tiền tệ kia.

Blockchain riêng tư: Một blockchain do một tổ chức duy nhất kiểm soát, thay vì phi tập trung.

Khóa riêng: Một đoạn dữ liệu bí mật chứng minh quyền của một người để chi tiêu bitcoin từ một ví cụ thể thông qua chữ ký mã hóa.

Bằng chứng cổ phần (PoS): Một cơ chế đồng thuận được sử dụng trong một số mạng blockchain, yêu cầu người dùng giữ một lượng nhất định tiền điện tử để tham gia xác nhận các giao dịch.

Bằng chứng công việc (PoW): Một cơ chế đồng thuận yêu cầu người dùng thực hiện một lượng công việc tính toán nhất định để có thể tham gia vào mạng lưới.

Blockchain công khai: Một blockchain mở cho bất kỳ ai tham gia và xác minh giao dịch, giúp hệ thống trở nên phi tập trung.

Khóa công khai: Một mã định danh duy nhất được dùng để nhận bitcoin, được tạo ra từ khóa riêng của người dùng thông qua một quá trình toán học.

Khóa công khai / Địa chỉ Bitcoin: Một chuỗi ký tự công khai (giống như mật khẩu nhận) được dùng để nhận bitcoin.

Sở cái công khai: Một cơ sở dữ liệu phi tập trung ghi lại công khai tất cả các giao dịch trên mạng Bitcoin.

Sức mua: Khả năng của tiền trong việc mua hàng hóa và dịch vụ.

Cụm từ khôi phục / Cụm từ seed: Một chuỗi gồm 12, 18 hoặc 24 từ dùng để tạo ra nhiều cặp khóa riêng và khóa công khai. Cụm từ này được dùng để khôi phục ví Bitcoin.

Tỷ lệ dự trữ bắt buộc: Tỷ lệ tiền gửi mà ngân hàng phải giữ lại dưới dạng dự trữ.

Ngân hàng bị hạn chế: Việc áp đặt các giới hạn hoặc hạn chế đối với dịch vụ ngân hàng hoặc quyền tiếp cận các dịch vụ ngân hàng.

Satoshi Nakamoto: Bí danh được sử dụng bởi người (hoặc nhóm người) ẩn danh đã tạo ra Bitcoin.

Satoshi: Đơn vị nhỏ nhất của Bitcoin, bằng 1/100.000.000 bitcoin. Đơn vị này được đặt theo tên của người sáng lập Bitcoin, Satoshi Nakamoto.

Satoshis trên mỗi byte (sat/b): Đơn vị dùng để đo phí giao dịch Bitcoin được tính trên mỗi byte dữ liệu giao dịch.

SegWit (Chữ ký tách biệt): Một bản nâng cấp giao thức của Bitcoin thay đổi cách dữ liệu được lưu trữ trên blockchain, giúp tăng dung lượng khối và giảm phí giao dịch.

Sidechain: Một blockchain được kết nối với một blockchain khác, cho phép chuyển tài sản hoặc thông tin giữa hai chuỗi.

Chữ ký: Một cơ chế toán học cho phép ai đó chứng minh quyền sở hữu.

Hợp đồng thông minh: Một hợp đồng tự động thực thi với các điều khoản của thỏa thuận được viết dưới dạng mã lập trình.

Soft Fork: Một thay đổi trong giao thức Bitcoin mà vẫn tương thích ngược với các phiên bản phần mềm cũ hơn.

Stablecoin: Một loại tiền mã hóa được thiết kế để duy trì giá trị ổn định, thường được neo theo đồng tiền pháp định hoặc tài sản khác.

Cung và cầu: Nguyên lý kinh tế cho rằng giá cả của hàng hóa hoặc dịch vụ được xác định bởi sự tương tác giữa lượng hàng hóa hoặc dịch vụ được cung cấp và lượng hàng hóa hoặc dịch vụ được nhu cầu.

Giá trị thời gian của tiền: Nguyên lý cho rằng tiền có giá trị cao hơn khi ở hiện tại so với tương lai.

Token: Một đơn vị giá trị được tạo ra trên blockchain, thường dùng để đại diện cho một tài sản hoặc tiện ích cụ thể trong một hệ sinh thái nhất định.

Token hóa: Quá trình tạo ra đại diện kỹ thuật số của một tài sản hoặc loại tài sản trên blockchain, cho phép sở hữu phân đoạn và chuyển nhượng dễ dàng.

Cặp giao dịch: Một cặp gồm hai đồng tiền hoặc tài sản có thể được giao dịch với nhau trên sàn giao dịch tiền mã hóa.

Phí giao dịch: Một khoản nhỏ bitcoin do người gửi thanh toán, nhằm khuyến khích các thợ đào bao gồm giao dịch đó vào khối và thêm nó vào blockchain.

Mã giao dịch: Một chuỗi các chữ số và chữ cái thể hiện chi tiết của một giao dịch Bitcoin (như số lượng gửi, địa chỉ người gửi và người nhận, cũng như ngày giao dịch) trên blockchain của Bitcoin.

Giao dịch: Quá trình chuyển bitcoin từ một địa chỉ này sang địa chỉ khác trên mạng Bitcoin.

Không cần tin cậy: Hệ thống hoặc giao dịch không yêu cầu phải tin tưởng vào bất kỳ bên thứ ba hay trung gian nào, mà dựa vào tính bảo mật và minh bạch của công nghệ nền tảng.

Bảng thuật ngữ

Xác thực hai yếu tố (2FA): Biện pháp bảo mật yêu cầu hai phương thức xác thực, thường là mật khẩu và một mã hoặc thiết bị riêng biệt, để truy cập tài khoản hoặc hoàn thành giao dịch.

Người không có tài khoản ngân hàng: Những cá nhân hoặc cộng đồng không có quyền truy cập vào các dịch vụ ngân hàng truyền thống.

Đơn vị hạch toán: Một đơn vị tiêu chuẩn dùng để biểu thị giá trị của hàng hóa và dịch vụ.

Biến động giá: Mức độ thay đổi của giá tài sản theo thời gian.

Địa chỉ ví: Một định danh duy nhất dùng để gửi và nhận bitcoin trên mạng lưới Bitcoin, thường được biểu diễn dưới dạng một chuỗi ký tự gồm chữ và số.

Sao lưu ví: Bản sao của khóa riêng và cụm từ khôi phục của ví Bitcoin, dùng để khôi phục quyền truy cập vào ví trong trường hợp ví gốc bị mất hoặc bị đánh cắp.

Ví: Một ví điện tử dùng để lưu trữ bitcoin, tương tự như ví vật lý. Ví này chứa khóa riêng cho phép bạn chỉ tiêu lượng bitcoin được phân bổ cho nó trên blockchain.

Cá voi: Cá nhân hoặc tổ chức nắm giữ một lượng lớn tiền mã hóa, có khả năng tác động đến giá thị trường thông qua các giao dịch lớn.

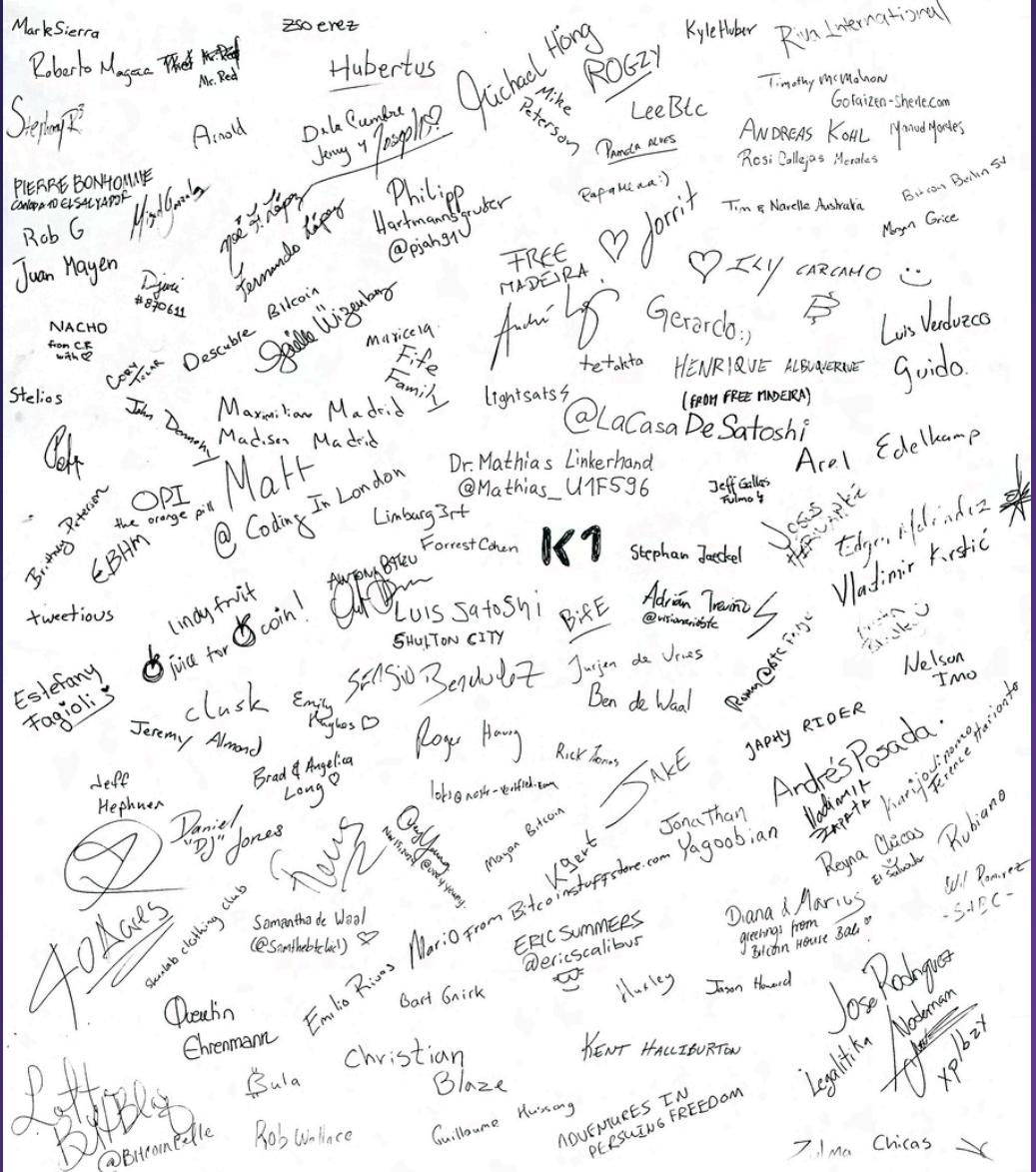
Hacker mũ trắng: Người hack có đạo đức, sử dụng kỹ năng của mình để phát hiện và khắc phục các lỗ hổng trong hệ thống máy tính và mạng.

Whitepaper: Tài liệu trình bày vấn đề mà một dự án blockchain hoặc tiền mã hóa đang cố gắng giải quyết, cùng với giải pháp mà dự án đề xuất.

XBT và BTC: Hai ký hiệu viết tắt đại diện cho bitcoin.

Độc lập là nhờ bạn!

CẢM ƠN CÁC NHÀ TÀI TRỢ ĐÃ
ĐÓNG GÓP CHO CHIẾN DỊCH
GEYSER CỦA CHÚNG TÔI HOẶC
TẠI SỰ KIỆN ADOPTING
BITCOIN 2024



Cảm ơn!



BITCOIN



Phiên Bản Tiếng Việt | 2025

Biên tập và lên kế hoạch: Seung-Goo Kang
Người dịch: Olivia Nguyễn

